ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

PRIVACY AS A PUBLIC GOOD: A PHILOSOPHICAL EXAMINATION OF DATA GOVERNANCE PRACTICES AMONG INDUSTRIAL SECURITY AGENCIES IN REGION IV-A, PHILIPPINES

Claur, Modesto T.
Philippine College of Criminology

Article DOI: https://doi.org/10.36713/epra31202
DOI No: 10.36713/epra31202

ABSTRACT

Privacy has increasingly emerged as a public good that extends beyond individual rights to encompass organizational accountability, public trust, and ethical governance. Within industrial security agencies, the growing reliance on personal data in security operations necessitates robust data governance practices that protect individuals while ensuring operational effectiveness. This study explored the lived experiences of industrial security personnel in implementing data governance practices, examining how privacy is understood and practiced as a public good among industrial security agencies in Region IV-A, Philippines. The study employed a qualitative phenomenological research design to capture the meanings and experiences of those directly involved in data governance implementation. Twenty-one informants, purposively selected from industrial security agencies in Region IV-A, participated in in-depth interviews. Data were analyzed using Braun and Clarke's thematic analysis to identify recurring patterns and essential themes that characterized participants' experiences. The findings revealed that data privacy governance has become an increasingly institutionalized component of daily security operations, with confidentiality, controlled access, proper records management, monitoring, and responsible information handling embedded in routine organizational practices. Informants associated effective privacy implementation with professionalism, accountability, ethical responsibility, and the preservation of client trust. Training programs, supervisory support, and organizational culture were identified as key mechanisms reinforcing privacy compliance. However, the study likewise uncovered persistent implementation challenges, including inconsistencies in policy application, varying levels of personnel awareness and competence, technological vulnerabilities, operational pressures, resource limitations, and the need to balance efficient security operations with privacy protection. Participants emphasized that effective data governance requires not only legal compliance but also sustained leadership commitment, continuous capacity building, adequate technological safeguards, systematic monitoring, and an organizational culture that recognizes privacy as a collective responsibility. Drawing from these findings, the study proposed a comprehensive Data Privacy Governance Policy designed specifically for industrial security agencies, which establishes standardized procedures for the lawful collection, processing, storage, access, disclosure, retention, and disposal of personal data while strengthening organizational accountability, privacy governance structures, training programs, monitoring mechanisms, and incident response protocols in accordance with the Data Privacy Act of 2012.

KEYWORDS: *Data privacy governance, public good, industrial security agencies, phenomenology, data governance, ethical governance, Data Privacy Act of 2012, Region IV-A, Philippines*

INTRODUCTION

Public safety governance today is increasingly shaped by data, digital technologies, and automated forms of decision-making. Across different jurisdictions, security agencies rely heavily on electronic records, surveillance systems, biometric technologies, intelligence databases, and information-sharing platforms to prevent crime, assess risks, and maintain public order. These technologies have changed not only how security institutions operate but also how state power is exercised. Authority is increasingly connected to the ability to collect, manage, analyze, and use information—an emerging form of governance that scholars describe as informational governance (Bennett & Raab, 2020; Floridi, 2020).

As the use of personal data expands, so does the importance of protecting privacy. Data privacy is not simply a matter of complying with laws and regulations. From a philosophical perspective, privacy is closely tied to personal autonomy, human dignity, and the freedom to make choices without unnecessary intrusion (Rössler, 2021; Stahl, 2022). This becomes particularly important when personal information is collected and processed by the state, especially by security institutions. These agencies exercise significant authority over individuals and often operate within hierarchical structures where decision-making may not always be fully visible to the public. Under such conditions, protecting personal information becomes more than an administrative responsibility; it becomes an ethical obligation.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

The growing use of surveillance and data analytics also brings an enduring tension between public security and individual freedom. Governments and security institutions may argue that extensive data collection is necessary to prevent crime, respond to threats, and protect communities. At the same time, excessive or poorly regulated collection of information can create opportunities for intrusion, weaken civil liberties, and reduce public accountability (Lyon, 2022; Zuboff, 2020). These concerns become particularly significant within security institutions, where operational demands, confidentiality, and strict chains of command can sometimes take precedence over ethical reflection and the protection of individual rights.

Although many countries have established data protection laws and regulatory frameworks, having rules in place does not necessarily mean that privacy is consistently respected in practice. Recent scholarship points to a continuing gap between formal compliance and the actual ethical use of personal information. Organizations may have privacy policies and procedures on paper while privacy principles remain weakly integrated into everyday decisions, organizational culture, and institutional governance (Gstrein & Beaulieu, 2022). This situation leads to an important philosophical question: Is following data protection laws enough to make an organization's use of personal information ethically acceptable?

In the Philippine context, this question has received relatively limited philosophical attention. Much of the existing discussion on data privacy focuses on legal requirements, technical safeguards, or administrative practices, while deeper questions about morality, responsibility, and human dignity are often given less attention. There remains a need to examine how security agencies understand privacy, how they justify the collection and use of personal information, and how they reconcile institutional responsibilities with their moral obligations toward individuals.

This study seeks to address this gap by examining data privacy not only as a matter of legal compliance but also as an ethical concern involving governance, authority, responsibility, and human dignity. By focusing on security agencies in Region IV-A (CALABARZON), the study provides a setting in which these philosophical questions can be explored in relation to actual institutional practices and experiences. In doing so, it aims to contribute to a deeper understanding of what it means to govern personal information responsibly in a security environment where the need to protect the public must be balanced with the equally important need to respect individual rights and dignity.

Theoretical Framework

This study is anchored in a set of interrelated theories and philosophical perspectives that collectively explain the ethical, institutional, and governance dimensions of data privacy within security agencies. Given the inherently coercive nature of security institutions and their expanding reliance on data-driven technologies, the theoretical framework integrates normative philosophy, governance theory, and institutional analysis to provide a comprehensive lens for examining data privacy practices. Specifically, the study is grounded in Information Ethics Theory, Social Contract Theory, Institutional Theory, and the Security–Privacy Trade-Off Framework.

Information Ethics Theory views information, particularly personal data, as having moral value because it affects human dignity, autonomy, and the ability of individuals to exercise meaningful choices (Floridi, 2020). From this perspective, data privacy is more than a legal or administrative requirement; it is an ethical responsibility grounded in respect for individuals. The theory provides a basis for examining whether security agencies use their informational power responsibly, transparently, and with proper regard for the rights and dignity of data subjects.

Further, Social Contract Theory emphasizes the reciprocal relationship between the state and its citizens. Citizens accept the authority of the state in exchange for protection of their rights and welfare, including privacy (Rössler, 2021). For security agencies, this means that access to personal information carries a corresponding responsibility to protect it from misuse, abuse, and unnecessary intrusion. This theory therefore helps examine whether data privacy practices strengthen public trust and uphold the legitimacy of state authority.

On the other hand, Institutional Theory provides another important perspective by explaining how organizational rules, culture, leadership, and resources influence actual institutional practices. Organizations may formally adopt privacy policies to comply with regulations or maintain legitimacy, yet implementation may vary because of established routines, resource limitations, or organizational practices (Bennett & Raab, 2020). This theory allows the study to look beyond formal compliance and examine the institutional factors that shape how data privacy is actually practiced within security agencies.

Finally, the study uses the Security–Privacy Trade-Off Framework to examine the tension between public safety and individual privacy. Security agencies often need access to personal information to prevent crime and address threats, but excessive surveillance or data collection may undermine individual rights and democratic safeguards (Lyon, 2022). Rather than viewing security and privacy as completely opposing interests, this framework encourages an examination of how agencies can pursue legitimate security objectives while still protecting privacy.

Taken together, these perspectives provide a comprehensive foundation for the study. Information Ethics Theory establishes the moral basis for responsible data use, Social Contract Theory connects privacy with state–citizen trust and legitimacy, Institutional Theory explains organizational practices and compliance, and the Security–Privacy Trade-Off Framework addresses the practical tension between security and privacy. Together, they guide the study in examining data privacy as not only a legal requirement but also an ethical and governance responsibility.

Statement of the Problem

This study examined data privacy governance and practice in security agencies in Region IV-A (CALABARZON), with particular focus on the handling of clients' personal data.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Specifically, it addressed the following research questions:

1. How do informants describe their experiences in implementing data privacy policies when handling clients' personal data?
2. How do informants within security agencies conceptualize data privacy in relation to their institutional mandates and the handling of clients' personal data?
3. What factors influence the implementation of data privacy policies concerning clients' personal data within security agencies?
4. How do data privacy practices in the handling of clients' personal data shape clients' perceptions of trust toward security agencies?
5. What policy framework may be proposed based on the findings of the study?

METHODOLOGY

This study employed a qualitative-phenomenological research design to explore the lived experiences of personnel in security agencies regarding data privacy governance and the handling of clients' personal data. As a qualitative approach, phenomenology focuses on understanding how individuals experience, interpret, and give meaning to a particular phenomenon. Creswell and Poth (2018) explained that phenomenology seeks to understand the common meaning of experiences shared by individuals, while Moustakas (1994) emphasized the discovery of the essence of a phenomenon based on the experiences of those who have directly encountered it.

The use of a qualitative-phenomenological design was appropriate because the study focused on the experiences, perceptions, interpretations, and meanings that security agency personnel attach to data privacy practices. Specifically, it assessed how informants experience the implementation of data privacy policies, how they perceive data privacy in relation to their institutional responsibilities, and what factors influence the implementation of these policies. It also explores how privacy practices are perceived to affect clients' trust and confidence in security agencies.

Through in-depth accounts and narratives, the design allowed informants to describe their experiences in their own words, providing a deeper understanding of the realities, challenges, and practices involved in protecting clients' personal data. The shared experiences of the informants can then be examined to identify common meanings, patterns, and themes that characterize data privacy governance within security agencies.

Table 1 presents the population of the study, which consists of 21 informants drawn from selected security agencies in Region IV-A (CALABARZON). The participants were purposively selected based on their direct involvement in the implementation, management, and operational handling of clients' personal data, ensuring that they possess relevant knowledge and experiences related to data privacy governance and practices.

Table 1. ***Population of the Study***

Group of Participants	Position/Role	Nature of Involvement in Data Privacy	Number of Participants
Security Agency Administrators	Commanders, Directors, Unit Heads	Policy oversight, leadership decisions, accountability	7
Data Privacy/ Records Officers	DPOs, Records Custodians, IT/Data Officers	Data handling, storage, access, compliance	7
Operational Personnel	Investigators, Intelligence Officers, Case Handlers	Operational use of personal and sensitive data	7
Total			21

The semi-structured interview guide was used as the primary data-gathering instrument to explore the informants' lived experiences and practices concerning data privacy governance in security agencies in Region IV-A (CALABARZON). The open-ended questions were aligned with the research questions and anchored on the Data Privacy Act of 2012 (Republic Act No. 10173) and relevant literature. Probing questions were included to clarify and deepen participants' responses regarding data privacy implementation, challenges, compliance, and its perceived influence on clients' trust. To establish content validity, the instrument was reviewed by three doctoral-level experts in research methodology, data privacy, ethics, or security governance. Their recommendations were incorporated into the final interview guide before its administration.

The thematic analysis following the six-phase framework of Braun and Clarke (2006) was utilized to systematically identify, analyze, and interpret patterns within participants' responses. The process involved familiarization with the transcribed data, generation of initial codes, identification and review of potential themes, definition and naming of themes, and production of the final report. Significant statements and recurring patterns related to data privacy governance and practices were coded and organized into themes, which were refined to ensure coherence and consistency with the dataset. Relevant participant quotations were incorporated to support the interpretation of findings. This approach enabled the researcher to derive meaningful insights into data privacy implementation, conceptual understanding, influencing factors, and its perceived impact on clients' trust in security agencies.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Ethical rigor was strictly observed throughout the research process. The study received approval from the Philippine College of Criminology Graduate School. Before participation, informed consent was obtained from all respondents, emphasizing voluntary participation, the right to withdraw, and the assurance of confidentiality. Data were anonymized and securely stored, with access limited to the researcher. No identifying information appeared in published outputs. The study adhered to the ethical principles of respect for persons, beneficence, and justice, as prescribed by the Data Privacy Act of 2012 (RA 10173) and institutional ethical guidelines.

RESULTS AND DISCUSSIONS

This section presents the findings on the data privacy governance and practice in security agencies in Region IV-A (CALABARZON), with particular focus on the handling of clients' personal data.

Informants' Lived Experiences in Implementing Data Privacy Policies when Handling Clients' Personal Data

Through the narratives of the 21 informants, this study provides a deeper understanding of how data privacy is practiced within the organizational setting and how personnel navigate the responsibilities associated with handling sensitive client information.

Table 2 presents the informants' experiences implementing data privacy policies when handling clients' personal data within their respective agencies. The findings reveal that data privacy has evolved from a mere regulatory requirement into an integral component of organizational operations, professional conduct, and service delivery. Informants consistently emphasized the importance of safeguarding personal information through established procedures, employee awareness programs, controlled access mechanisms, and continuous compliance monitoring.

Moreover, the findings demonstrate that effective implementation of data privacy policies contributes not only to information security but also to strengthening client trust and organizational credibility. Six major themes emerged from the analysis: Institutionalization of Data Privacy in Daily Operations, Culture of Confidentiality and Professional Responsibility, Privacy Awareness and Capacity Development, Controlled Access and Responsible Information Sharing, Compliance Monitoring and Accountability Mechanisms, and Integration of Privacy Protection with Organizational Trust and Security Functions.

Theme 1: Institutionalization of Data Privacy in Daily Operations. This reflects informants' experiences that data privacy has become integrated into routine organizational activities, particularly in the collection, storage, processing, and disposal of personal information. This finding is consistent with Afzal and Panagiotopoulos (2025) and the OECD (2024), which emphasize that privacy protection should be embedded in organizational systems and operational processes rather than treated as a separate administrative function. In the Philippine context, the National Privacy Commission (NPC, 2022; 2023; 2024; 2025) likewise promotes the integration of privacy requirements into organizational policies, procedures, and technologies. These sources support the informants' experiences that data privacy has become a regular and institutionalized component of agency operations.

Theme 2: Culture of Confidentiality and Professional Responsibility. This demonstrates that privacy protection is reinforced through professional ethics, organizational values, and employee accountability. This finding is consistent with the Information Commissioner's Office (2025), which emphasized that effective privacy compliance requires not only formal policies but also organizational discipline and employee commitment to responsible data handling. The 2024 systematic review likewise emphasized the importance of privacy, security, and confidentiality safeguards in protecting personal information and strengthening trust in data-handling practices. In the Philippine context, Sancon (2023) found that effective privacy governance is associated with organizational commitment and accountability mechanisms. The informants' responses therefore suggest that confidentiality has become an integral part of professional conduct and organizational culture.

Theme 3: Privacy Awareness and Capacity Development. This highlights the importance of orientations, seminars, and continuous training in strengthening employees' understanding and practice of privacy responsibilities. This finding is consistent with Miano (2025) and Ayuyang and Ayuyang (2024), who found that employee awareness is associated with effective data management, privacy, and cybersecurity practices. Agup (2024) likewise emphasized the continuing need for training even among organizations with high levels of compliance. The OECD (2024) further stressed that effective privacy governance requires personnel with adequate knowledge and capacity to implement data protection obligations. These findings support the informants' experiences that sustained training and awareness programs help develop privacy-conscious behavior among personnel.

Theme 4: Controlled Access and Responsible Information Sharing. This highlights the importance of limiting access to personal data to authorized personnel and ensuring that information is disclosed only for lawful and legitimate purposes. This finding is consistent with the European Data Protection Board (2026) and the Information Commissioner's Office (ICO), which emphasize access controls, accountability, and privacy by design and default. Sunde (2023) likewise highlighted the principle of purpose limitation, whereby personal information should only be used for its intended purpose. Philippine privacy notices and operational guidelines similarly emphasize authorized access, identity verification, and controlled disclosure. These findings support the informants' experiences that clear access controls and defined permissions are essential to responsible handling of personal information.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Theme 5: Compliance Monitoring and Accountability Mechanisms. This emphasizes the importance of supervision, audits, compliance checks, and enforcement in ensuring adherence to data privacy policies. This finding is consistent with the European Data Protection Board (2026) and the Information Commissioner's Office (2025), which identified accountability and effective monitoring as essential components of privacy governance. Sancon (2023) likewise emphasized the contribution of accountability structures to effective privacy management, while Dela Rosa (2025) noted that privacy awareness alone does not ensure compliance without adequate oversight. These findings support the informants' experiences that continuous monitoring and accountability mechanisms are necessary to sustain compliance with established privacy policies.

Table 2. ***Experiences of the Informants in Implementing Data Privacy Policies when Handling Clients' Personal Data***

Interview Question	Actual Responses	Themes
Can you describe your experiences in implementing data privacy policies when handling clients' personal data in your agency?	"Implementing data privacy policies has become an important part of our daily operations." (Administrator 1) "My role requires me to monitor the collection, storage, and disposal of records." (Officer 1) "I handle reports that contain personal details. We are required to secure these documents." (Personnel 4)	Theme 1. Institutionalization of Data Privacy in Daily Operations
	"We developed a culture where confidentiality is emphasized in every department." (Administrator 1) "I often remind employees about confidentiality obligations and proper data handling procedures." (Officer 5) "Protecting client data is part of maintaining professionalism." (Personnel 6) "We were instructed to keep these records confidential." (Personnel 1)	Theme 2. Culture of Confidentiality and Professional Responsibility
	"After conducting orientations, I observed greater awareness and responsibility among employees." (Administrator 2) "Awareness among personnel is improving, although continuous education remains necessary." (Officer 2) "These incidents highlighted the importance of training and policy reinforcement." (Officer 3) "After attending seminars, I became more conscious of the importance of protecting client information." (Personnel 3)	Theme 3. Privacy Awareness and Capacity Development
	"We need immediate access to information during security operations, but we must also ensure that only authorized personnel can access client data." (Administrator 3) "Implementing privacy policies helped establish clear procedures on who can access records." (Administrator 5) "I ensure that access permissions are granted only to authorized personnel." (Officer 4) "Data privacy policies help establish clear boundaries regarding who may access information." (Personnel 7)	Theme 4. Controlled Access and Responsible Information Sharing
	"Data privacy implementation requires constant supervision." (Administrator 4)	Theme 5. Compliance Monitoring and Accountability Mechanisms

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

	"My experience includes conducting compliance checks and reviewing data processing activities." (Officer 6) "Employees become more cautious when they understand the consequences of improper data handling." (Officer 7) "We follow procedures to ensure that documents are submitted only to authorized offices." (Personnel 2)	
	"Personal information is processed only for legitimate purposes." (Officer 1) "We make sure that records are used only for official purposes." (Personnel 5)	Theme 6. Integration of Privacy Protection with Organizational Trust and Security Functions

Theme 6: Integration of Privacy Protection with Organizational Trust and Security Functions. This demonstrates that effective data privacy protection contributes to organizational security, public trust, and institutional legitimacy. This finding is consistent with Bradford et al. (2020) and Li (2024), who emphasized that responsible and transparent use of privacy-sensitive technologies strengthens public trust and acceptance of data-driven systems. Guazzo et al. (2026) found that trust in government implementation can reduce privacy concerns and increase general acceptance of video-based information-processing technologies. In the Philippine context, Dausan et al. (2025), Espiel (2024), and Kiram et al. (2024) similarly highlighted the importance of security, transparency, accountability, and privacy governance in building trust in police and other institutions. These findings support the informants' experiences that privacy protection enhances both client trust and organizational security.

The findings also support the study's theoretical foundations. Information Ethics Theory is reflected in the emphasis on confidentiality, ethical responsibility, and respect for personal information; Social Contract Theory in the relationship between responsible data handling, trust, and institutional legitimacy; Institutional Theory in the integration of privacy practices into organizational routines through policies, training, monitoring, and governance; and the Security–Privacy Trade-Off Framework in balancing operational security requirements with privacy protection through controlled access and responsible information sharing. Collectively, the findings indicate that data privacy implementation is a governance practice shaped by ethical principles, organizational culture, personnel capacity, and accountability mechanisms. Compliance with the Data Privacy Act of 2012 therefore extends beyond regulatory adherence by contributing to public trust, ethical governance, and rights-respecting security operations.

Synthesis of the Findings. Overall, effective data privacy implementation is supported by the integration of privacy practices into daily operations, a culture of confidentiality, continuous personnel development, controlled access and information sharing, and sustained compliance monitoring. These findings demonstrate that protecting clients' personal information requires not only policies and procedures but also competent personnel, organizational commitment, and effective accountability mechanisms.

Informants' Conceptualization of Data Privacy in Relation to Institutional Mandates and the Handling of Clients' Personal Data

This section presents the findings related to participants' understanding of data privacy, its connection to the mandate and responsibilities of security agencies, and the ways in which operational functions can be balanced with the protection of clients' personal information. Through the perspectives of Administrators, Data Privacy/Records Officers, and Operational Personnel, the study explores how data privacy is conceptualized and integrated into the professional responsibilities and operational practices of security agencies.

Understanding of Data Privacy in the Context of Security Agency Work. Table 3 presents the informants' understanding and definition of data privacy within the context of their work in a security agency. The findings reveal that data privacy is perceived as a multifaceted responsibility encompassing the protection of confidential information, accountability in handling personal data, compliance with legal and regulatory requirements, and the preservation of client trust. Informants consistently associated data privacy with safeguarding sensitive records against unauthorized access, ensuring responsible information management, adhering to established laws and policies, and maintaining professionalism in service delivery. These perspectives demonstrate that data privacy is not viewed merely as a technical or legal requirement but as an essential component of ethical and professional practice within security agencies. From the responses, four major themes emerged: Protection of Confidential Information, Accountability in Information Handling, Legal and Regulatory Compliance, and Building Trust and Professional Integrity.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Table 3. ***Understanding and Definition of Data Privacy in a Security Agency Context***

Interview Question	Actual Responses	Themes
How do you understand or define data privacy in the context of your work in a security agency?	"Data privacy means protecting clients' personal information from unauthorized access or disclosure." (Administrator 1) "It refers to safeguarding records and ensuring that information is used only for legitimate purposes." (Officer 2) "It means keeping confidential information secure and sharing it only with authorized persons." (Personnel 3) "We are responsible for securing all client records from unauthorized use." (Officer 1) "Data privacy is part of our accountability in handling sensitive information." (Administrator 4)	Protection of Confidential Information
	"Data privacy is a responsibility that comes with handling sensitive information." (Administrator 4) "It is about accountability in processing, storing, and sharing personal data." (Officer 5) "It reminds us to be responsible when dealing with client records." (Personnel 6) "Every personnel must be accountable for the data they handle." (Officer 3)	Accountability in Information Handling
	"It is a legal obligation that our agency must comply with." (Administrator 2) "Data privacy is compliance with policies, regulations, and established procedures." (Officer 1) "It means following rules on how personal information should be collected and protected." (Personnel 1) "We strictly follow the Data Privacy Act and related guidelines." (Administrator 6)	Legal and Regulatory Compliance
	"It helps maintain the trust of our clients." (Administrator 7) "Data privacy assures clients that their information is safe with us." (Officer 7) "Protecting personal data shows professionalism and respect for clients." (Personnel 5) "Clients become more confident when their information is properly handled." (Officer 6)	Building Trust and Professional Integrity

Theme 1: Protection of Confidential Information. This reflects the informants' understanding that data privacy primarily involves safeguarding personal information from unauthorized access, disclosure, misuse, and exploitation. This finding is consistent with Jung (2024), the Information Commissioner's Office (ICO), and the European Data Protection Board (2026), which emphasize confidentiality, appropriate access controls, and safeguards throughout the data-processing lifecycle, particularly in law-enforcement and security contexts. In the Philippine setting, the National Privacy Commission (NPC, 2024; 2025) likewise emphasizes organizational, physical, and technical measures to prevent unauthorized access and disclosure. These findings support the informants' view that protecting confidential information is a fundamental component of data privacy.

Theme 2: Accountability in Information Handling. This highlights the informants' view that personnel are personally and professionally responsible for the proper processing, storage, sharing, and protection of personal information. This finding is consistent with the OECD (2024) and European Data Protection

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Board (2026), which identify accountability as a core principle of effective data governance and lawful data processing. In the Philippine context, Sancon (2023) and Kiram et al. (2024) likewise emphasized the importance of accountability mechanisms in strengthening privacy governance and trustworthy data management. These findings indicate that data privacy is perceived not merely as a technical safeguard but also as an ethical and professional responsibility.

Theme 3: Legal and Regulatory Compliance. This reflects the informants' perception that data privacy requires adherence to laws, regulations, policies, and established procedures governing the processing of personal information. This finding is consistent with the OECD (2024) and European Data Protection Board (2026), which emphasize that privacy governance must operate within applicable legal frameworks and safeguards. The Information Commissioner's Office (ICO) likewise recognizes privacy compliance as an organizational obligation requiring adherence to regulatory requirements and documented procedures. In the Philippine context, the National Privacy Commission (NPC, 2022; 2023; 2024; 2025) and the Data Privacy Act of 2012 provide the legal standards governing personal data processing. These findings support the informants' understanding of data privacy as both a legal and organizational obligation.

Theme 4: Building Trust and Professional Integrity. This highlights the informants' belief that protecting personal information strengthens client confidence, demonstrates professionalism, and enhances institutional credibility. This finding is consistent with Bradford et al. (2020) and Li (2024), who emphasized that responsible and privacy-conscious data practices contribute to public trust and acceptance of data-driven systems. Guazzo et al. (2026) likewise found that institutional trust can reduce privacy concerns and increase acceptance of information-processing practices. In the Philippine context, Dausan et al. (2025), Espiel (2024), and Kiram et al. (2024) similarly identified transparency, security, accountability, and privacy governance as important factors in strengthening public trust and institutional legitimacy. These findings support the informants' view that data privacy extends beyond regulatory compliance to include professional integrity and trust-building.

Synthesis of the Findings. Overall, the findings indicate that security agency personnel understand data privacy as encompassing the protection of confidential information, accountability in information handling, compliance with legal and regulatory requirements, and the promotion of trust and professional integrity. These interconnected dimensions demonstrate that data privacy is both an organizational obligation and an ethical responsibility that supports effective service delivery, information security, and stakeholder confidence. Strengthening awareness of these dimensions may further promote privacy compliance, professional conduct, and institutional credibility in managing sensitive personal information.

Balancing Operational Functions and the Protection of Clients' Personal Data. Table 4 presents the informants' views on how a security agency should balance its operational functions with the protection of clients' personal data. The findings indicate that respondents recognize the inherent tension between operational efficiency and strict data privacy compliance, particularly in fast-paced or urgent security situations. However, they consistently emphasize that operational demands should never override the obligation to safeguard personal information. The responses highlight the importance of necessity-based access, clear policies and procedures, continuous capacity building, the use of technology, and the integration of privacy considerations into all operational decisions.

The findings reveal five interconnected themes describing how security agency personnel balance operational efficiency with data privacy. First, the Principle of Necessity and Limited Access shows that access to personal information is restricted to data necessary for legitimate work purposes. This minimizes unnecessary exposure and supports confidentiality, consistent with the Data Privacy Act of 2012. Sunde (2023) emphasized the principles of purpose limitation and purpose orientation in the subsequent use of data by police, highlighting the need to restrict the use of personal information to legitimate and relevant purposes. This perspective complements Information Ethics Theory and the Security–Privacy Trade-Off Framework, which emphasize respecting individual privacy while recognizing legitimate operational and security needs.

Second, Implementation of Clear Policies and Procedures demonstrates that defined access rules and standardized protocols provide personnel with clear guidance for handling personal information during routine and high-pressure operations. Clear procedures reduce ambiguity, promote accountability, and support consistent decision-making. This finding is consistent with Institutional Theory and studies emphasizing the importance of organizational structures, policies, and coordination mechanisms in effective data governance.

Third, Capacity Building and Privacy Awareness highlights the importance of continuous training, orientations, and reminders in enabling personnel to apply privacy principles while performing operational duties. Training strengthens decision-making, reinforces compliance, and helps personnel manage competing demands between efficiency and confidentiality. This finding is supported by Ayuyang and Ayuyang (2024), Agup (2024), and Herrewijnen et al. (2024), which emphasize employee awareness and continuous learning as important factors in privacy compliance.

Fourth, Use of Security Technologies to Support Privacy Protection illustrates how access controls, monitoring systems, and secure digital platforms can simultaneously enhance operational efficiency and protect personal information. Appropriate technological safeguards reduce unauthorized access, human error, and privacy risks while supporting efficient information management. This finding is consistent with Donatz-Fest (2024), Neiva et al. (2023), and Casaburo and Marsh (2024), as well as the security requirements of the Data Privacy Act and related National Privacy Commission issuances.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Table 4. ***Balancing Operational Functions and the Protection of Clients' Personal Data***

Interview Question	Actual Responses	Themes
In your view, how should a security agency balance its operational functions with the protection of clients' personal data?	"Operational needs should not compromise data privacy." (Administrator 1) "Information should only be accessed when necessary for legitimate work purposes." (Officer 2) "We should only use the information required to perform our duties." (Personnel 5) "Even during urgent operations, confidentiality must still be observed." (Officer 1)	Principle of Necessity and Limited Access
	"Policies must clearly define who can access information during operations." (Administrator 4) "There should be procedures that allow operational efficiency without exposing sensitive records." (Officer 5) "Following established protocols helps prevent misuse of information." (Personnel 7) "Clear guidelines help avoid confusion in handling data during operations." (Officer 3)	Implementation of Clear Policies and Procedures
	"Continuous training is needed so personnel understand both operational and privacy requirements." (Administrator 2) "Awareness programs help employees make proper decisions when handling data." (Officer 1) "Regular reminders help us stay compliant even during busy operations." (Personnel 3) "Training improves how we balance speed and confidentiality." (Officer 6)	Capacity Building and Privacy Awareness
	"Technology can help us achieve both security and privacy objectives." (Administrator 6) "Access controls and monitoring systems reduce risks while supporting operations." (Officer 6) "Secure systems make it easier to protect information while performing our duties." (Personnel 6) "Digital tools help prevent unauthorized access during operations." (Officer 4)	Use of Security Technologies to Support Privacy Protection
	"The agency must ensure operational effectiveness while preserving client trust." (Administrator 7) "Privacy protection should be considered in every operational decision." (Officer 7) "Protecting information is part of providing quality security service." (Personnel 2) "Balancing efficiency and confidentiality are essential in our work." (Officer 2)	Balancing Service Delivery with Privacy Protection

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Fifth, Balancing Service Delivery with Privacy Protection represents the overarching finding that privacy should be integrated into operational decision-making rather than treated as a separate concern. Informants viewed confidentiality, service quality, and client trust as interconnected objectives. This finding is supported by the Security–Privacy Trade-Off Framework and Social Contract Theory, as well as Li (2024), Sagana (2025), Guler (2025), and Nieuwenhuizen et al. (2025), which emphasize that fair, transparent, and accountable privacy practices strengthen institutional trust.

Overall, the findings demonstrate that balancing operational efficiency and data privacy requires more than compliance with formal rules. It involves limited and purpose-based access, clear organizational procedures, continuous personnel development, appropriate technological safeguards, and privacy-conscious service delivery. These mechanisms enable security agencies to pursue operational objectives while protecting personal information, maintaining professional accountability, and strengthening client trust and institutional legitimacy.

Factors Influencing the Implementation of Data Privacy Policies Concerning Clients' Personal Data in Security Agencies

Internal Factors Influencing the Implementation of Data Privacy Policies Within Security Agencies. Based on the interviews conducted, there are internal factors that influence the implementation of data privacy policies within the agency. The findings indicate that effective implementation is shaped not only by formal rules and regulations but also by internal organizational dynamics such as leadership support, employee competence, policy clarity, resource availability, workplace culture, and enforcement mechanisms. These factors collectively determine how well data privacy policies are understood, accepted, and practiced by personnel in their daily operations. The responses highlight that successful data privacy implementation requires a supportive organizational environment where systems, people, and leadership work together to ensure compliance.

The findings identified six interconnected themes that influence the implementation of data privacy policies within security agencies. First, **Leadership Commitment and Supervisory Support** demonstrate that management plays a central role in translating privacy policies into organizational practice. Visible leadership, consistent guidance, and supervisory reinforcement strengthen accountability and encourage personnel to adhere to privacy standards. This finding is supported by Institutional Theory and studies by Tano (2024) and Donatz-Fest (2024), which emphasize the influence of leadership and managerial decisions on privacy and data governance practices.

Second, **Knowledge, Training, and Awareness** highlight the importance of continuous education in developing personnel competence and improving compliance. Regular training, seminars, and orientations help employees understand their privacy responsibilities, reduce knowledge gaps, and make appropriate decisions when handling personal information. This finding is supported by Ayuyang and Ayuyang (2024), Agup (2024), and Herrewijnen et al. (2024) and is consistent with Information Ethics Theory, which emphasizes awareness of the ethical responsibilities involved in handling personal information.

Third, **Clarity of Policies and Procedures** indicates that clearly documented and communicated guidelines provide personnel with direction and reduce ambiguity in data handling. Standard operating procedures promote consistency, minimize errors, and support uniform compliance. This finding aligns with Institutional Theory and studies by Jones et al. (2024) and the Information Commissioner's Office, which emphasize that unclear procedures and inadequate guidance can hinder privacy compliance.

Fourth, **Availability of Organizational Resources and Technology** demonstrates that adequate technological infrastructure and resources are essential for effective privacy implementation. Secure databases, access controls, and monitoring systems strengthen data protection and reduce risks associated with manual processes and human error. This finding is supported by Donatz-Fest (2024) and Galang and Villa-Buena (2024), whose study highlighted the importance of organizational, physical, and technical measures in the processing and protection of personal data. It is also consistent with the security safeguards required under the Data Privacy Act of 2012 and relevant National Privacy Commission issuances.

Fifth, **Culture of Privacy and Confidentiality** shows that shared organizational values and norms influence how privacy responsibilities are practiced within the agency. When confidentiality and responsible data handling are embedded in organizational practices, employees are more likely to consistently observe privacy responsibilities. This finding is consistent with Institutional Theory and Information Ethics Theory and is supported by Camorongan (2023), who emphasized the importance of transparency, accountability mechanisms, and responsible data governance in strengthening institutions.

Fifth, **Culture of Privacy and Confidentiality** shows that shared organizational values and norms significantly influence how privacy policies are practiced. When confidentiality becomes embedded in organizational culture, employees are more likely to internalize privacy responsibilities and consistently protect personal information. This finding supports Institutional Theory and Information Ethics Theory, as well as the findings of Donatz-Fest (2024), and is supported by Camorongan (2023), who emphasized the importance of transparency, accountability mechanisms, and responsible data governance in strengthening institutions.

Sixth, **Monitoring, Compliance, and Enforcement Mechanisms** emphasize the importance of audits, supervision, compliance checks, and enforcement in sustaining privacy implementation. These mechanisms reinforce accountability, identify gaps, and encourage corrective action. The finding is consistent with the Data Privacy Act of 2012, National Privacy Commission guidelines, and Information Commissioner's Office audits, while Institutional Theory explains how monitoring reinforces organizational norms and Social Contract Theory highlights its role in maintaining public trust.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Overall, the findings indicate that effective data privacy implementation is shaped by the interaction of leadership, personnel competence, policy clarity, organizational resources and technology, privacy-oriented culture, and accountability mechanisms. These factors demonstrate that privacy compliance cannot depend solely on formal policies; it requires sustained leadership support, capable personnel, adequate resources, shared organizational values, and continuous monitoring and enforcement. Together, these elements strengthen the consistent and accountable protection of personal information within security agencies.

External Factors Influencing Data Privacy Practices in Security Agencies. The implementation of data privacy practices within the agency is influenced not only by internal mechanisms but also by external factors. These include legal and regulatory requirements, client expectations, technological developments, industry standards, cybersecurity threats, and public scrutiny. These factors continuously shape the agency's data privacy practices and encourage stronger protection of personal information. The findings indicate that data privacy compliance is a dynamic process influenced by changing laws, emerging risks, and growing societal expectations.

The findings identified six major external factors influencing the implementation of data privacy practices in security agencies. First, **Legal and Regulatory Requirements** emerged as a primary external driver, with the Data Privacy Act and other government regulations providing the legal foundation for organizational privacy policies and procedures. Compliance with these requirements promotes standardization, accountability, and institutional legitimacy. This finding is consistent with the OECD (2024), European Data Protection Board (2026), and National Privacy Commission (NPC, 2022–2025), which emphasize the mandatory nature of legal and regulatory compliance in personal data processing.

Second, **Client Expectations and Trust Requirements** demonstrate that clients' demand for confidentiality, security, and assurance influences agencies to strengthen privacy safeguards. Maintaining client trust encourages continuous improvement in data protection practices and enhances organizational credibility. This finding is supported by Bradford et al. (2020), Li (2024), Guazzo et al. (2026), Dausan et al. (2025), and Kiram et al. (2024), which highlight the relationship between privacy protection, accountability, transparency, and institutional trust.

Third, **Technological Developments and Emerging Risks** highlight the dual role of technology as both an enabler of operational efficiency and a source of emerging privacy vulnerabilities. Rapid digital transformation requires agencies to continuously update systems, strengthen cybersecurity, and adapt to new threats. This finding is supported by Afzal and Panagiotopoulos (2025), Obendiek (2025), Spyropoulos and Tsiantos (2025), Espiel (2024), and Andaya et al. (2025), who emphasize the growing governance and cybersecurity challenges associated with digital systems.

Fourth, **Industry Standards and Professional Expectations** show that agencies are influenced by professional norms, recognized security standards, and benchmarking practices. Aligning privacy procedures with established standards promotes consistency, accountability, and continuous improvement. This finding is consistent with the OECD (2024), European Data Protection Board (2026), and National Privacy Commission (2024), which emphasize governance frameworks, regulatory compliance, security measures, and responsible data protection.

Fifth, **Cybersecurity Threats and Environmental Pressures** indicate that evolving cyber threats and broader security risks encourage agencies to strengthen safeguards and remain vigilant. Continuous risk assessment, monitoring, and proactive security measures are necessary to address changing threats and protect personal information. This finding is consistent with the National Privacy Commission's requirements for security controls, access management, privacy management programs, personnel training, and business continuity measures.

Sixth, **Public Scrutiny and Social Accountability Pressures** demonstrate that public awareness, transparency, and institutional accountability can influence how organizations implement data protection practices. Concerns regarding reputational damage and loss of public trust encourage agencies to strengthen transparency, accountability, and responsible data governance. This perspective is consistent with the OECD (2024), which recognizes privacy as important to trust in the collection and use of data, and with the National Privacy Commission's emphasis on empowering data subjects to identify organizations they can trust.

Overall, the findings demonstrate that data privacy implementation is shaped not only by internal organizational conditions but also by the legal, social, technological, professional, and security environment in which agencies operate. Effective privacy governance therefore requires agencies to remain responsive to regulatory requirements, client expectations, technological developments, professional standards, cybersecurity threats, and public accountability pressures. These external factors collectively encourage continuous improvement and strengthen the agencies' capacity to protect personal information while maintaining public trust and operational effectiveness.

Data Privacy Practices and Their Influence on Clients' Trust in Security Agencies

Table 5 presents the effects of data privacy practices on clients' trust in the agency. The findings indicate that effective data privacy practices strengthen client confidence, enhance organizational credibility, promote long-term relationships, support transparency, and reduce reputational risks. Informants emphasized that clients are more willing to cooperate and engage with the agency when they are assured that their personal information is handled confidentially and responsibly. These findings demonstrate that data privacy extends beyond regulatory compliance and operational requirements, serving as a critical factor in building and sustaining client trust and confidence in service delivery.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Table 5. ***Data Privacy Practices and Their Influence on Clients' Trust in Security Agencies***

Interview Question	Actual Responses	Themes
Based on your observation, how do data privacy practices affect clients' trust in your agency?	"Clients are more willing to share necessary information when they know their data are protected." (Admin 1) "Clients cooperate more when privacy safeguards are clearly explained." (Officer 2) "Clients feel more comfortable providing personal information when they trust our procedures." (Personnel 3) "Trust increases when confidentiality is consistently observed." (Officer 1)	Enhanced Client Confidence Through Data Protection
	"Strong privacy practices strengthen our professional image." (Admin 5) "Compliance demonstrates organizational responsibility." (Officer 4) "Clients view the agency as more reliable when information is handled properly." (Personnel 6) "Proper data handling improves credibility." (Officer 3)	Professionalism and Organizational Credibility
	"Protecting personal data helps establish long-term relationships with clients." (Admin 7) "Trust grows when clients consistently see confidentiality." (Officer 7) "Clients remain loyal when privacy is respected." (Personnel 5) "Consistency in privacy builds long-term trust." (Officer 6)	Trust as a Foundation for Long-Term Client Relationships
	"Privacy compliance reassures clients that we operate responsibly." (Admin 2) "Clients appreciate transparency in how information is processed." (Officer 1) "Clear privacy procedures give clients peace of mind." (Personnel 1) "Transparency strengthens client confidence." (Officer 5)	Transparency and Assurance in Service Delivery
	"Strict privacy implementation reduces complaints and concerns." (Admin 6) "Good data protection reduces reputational risks." (Officer 6) "Avoiding data leaks maintains trust." (Personnel 7) "Strong safeguards prevent negative perceptions." (Officer 2)	Risk Reduction and Trust Protection

The findings identified five interconnected themes demonstrating how data privacy practices influence clients' trust in security agencies. First, **Enhanced Client Confidence Through Data Protection** shows that effective privacy safeguards increase clients' willingness to provide necessary information and cooperate with the agency. Consistent confidentiality reduces concerns about misuse or unauthorized disclosure and strengthens clients' sense of security. This finding is supported by Information Ethics Theory, particularly the principles of respect for autonomy and informational privacy, and by Bradford et al. (2020), Li (2024), and Guler (2025), who linked responsible data handling and perceived fairness with greater trust and acceptance.

Second, **Professionalism and Organizational Credibility** indicates that proper data handling enhances the agency's professional image and demonstrates organizational responsibility. Compliance with privacy standards signals reliability, competence, and institutional integrity. This finding is consistent with Institutional Theory, which links organizational legitimacy to conformity with established norms, and Social Contract Theory, which emphasizes institutional responsibility to protect individual rights.

Third, **Trust as a Foundation for Long-Term Client Relationships** demonstrates that trust develops through consistent and repeated experiences of confidentiality and responsible data handling. Sustained privacy practices encourage

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

client loyalty, continued engagement, and stronger agency-client relationships. This finding is supported by Guazzo et al. (2026) and Nieuwenhuizen et al. (2024), who found that providing explanations about police algorithmic systems increased citizen trust, highlighting the importance of transparency and explainability in fostering confidence in information-processing practices.

Fourth, **Transparency and Assurance in Service Delivery** highlights that clear communication regarding privacy procedures and data handling reassures clients and reduces uncertainty. Transparency strengthens accountability and enables clients to understand how their information is processed and protected. This finding is consistent with Information Ethics Theory, the OECD (2024), and the Information Commissioner's Office (2025), which emphasize transparency and responsible communication as important elements of trustworthy data governance.

Fifth, **Risk Reduction and Trust Protection** demonstrates that effective privacy safeguards reduce complaints, data breaches, reputational risks, and negative perceptions that may undermine client confidence. Strong data protection therefore serves both information-security and trust-preservation functions. This finding is supported by the European Data Protection Board (2026), Dasgupta et al. (2025), and Jones et al. (2024), which emphasize accountability, transparency, and effective data governance as mechanisms for reducing privacy and institutional risks.

Overall, the findings demonstrate that data privacy practices extend beyond regulatory compliance and directly contribute to client confidence, organizational credibility, long-term relationships, transparency, and risk reduction. Effective privacy protection strengthens the agency's ability to build and sustain trust by demonstrating responsible data stewardship, professional integrity, and accountability. Thus, data privacy should be regarded not only as a legal and operational obligation but also as a strategic component of trustworthy and effective service delivery.

Proposed Data Privacy Policy Framework for Security Agencies

The **Proposed Data Privacy Governance Policy** was developed directly from the four major findings of the study and translates the informants' experiences, perceptions, and identified needs into a practical institutional framework for managing personal data in industrial security agencies. The policy addresses the operational, ethical, legal, and organizational concerns identified in the study while promoting regulatory compliance, effective data governance, and client trust.

The **first finding**, which revealed that data privacy has become institutionalized in daily security operations but remains affected by human error, inconsistent compliance, operational pressures, technological vulnerabilities, and resource limitations, provides the basis for provisions on **standard operating procedures, personnel responsibilities, records management, cybersecurity, monitoring, auditing, incident reporting, and sanctions**. The **second finding**, which established that data privacy is understood as both a legal obligation and an ethical responsibility, is reflected in the **Policy Declaration, Governing Principles, Confidentiality and**

Ethical Conduct Policy, and Privacy Governance Responsibilities.

The **third finding**, which identified internal and external factors influencing implementation—including leadership support, personnel competence, organizational culture, policy clarity, technology, legal requirements, cybersecurity threats, client expectations, and regulatory oversight—supports provisions on **management responsibilities, designation of a Data Protection Officer, personnel training, client coordination, cybersecurity safeguards, compliance monitoring, audits, and periodic policy review**. The **fourth finding**, which demonstrated the influence of privacy practices on client trust, organizational credibility, and professional reputation, provides the basis for provisions on **confidentiality, secure data handling, authorized disclosure, transparency, breach response, and accountability** throughout the data lifecycle.

Overall, the proposed policy operationalizes the study's findings by providing a comprehensive framework that strengthens **privacy protection, organizational accountability, ethical and legal compliance, and client trust**. It bridges the gap between the lived experiences of industrial security personnel and standardized data governance practices while supporting effective security operations and compliance with the **Data Privacy Act of 2012 (Republic Act No. 10173)**. As a practical and sustainable output, the policy seeks to enhance data governance and protect clients' personal information within industrial security agencies in Region IV-A, Philippines.

The proposed **Data Privacy Governance Policy** is primarily recommended for adoption by the **management of private security agencies**, particularly agency owners, presidents, chief executive officers, operations managers, and **Data Protection Officers (DPOs)** responsible for establishing policies, ensuring compliance with **Republic Act No. 10173 or the Data Privacy Act of 2012**, and promoting a culture of data privacy. The policy is likewise intended for all agency personnel, including supervisors, detachment commanders, investigators, security guards, records custodians, administrative staff, and other employees who process personal data in the performance of their duties. **Clients and partner organizations** may use the policy as a reference for aligning contractual privacy obligations and information security practices. **Regulatory bodies**, particularly the **National Privacy Commission (NPC)** and the **Philippine National Police–Supervisory Office for Security and Investigation Agencies (PNP-SOSIA)**, may also consider the policy as a reference for promoting standardized data privacy practices among licensed private security agencies.

Conclusions

With the findings derived from the study, the following are concluded:

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Data privacy policy implementation in security agencies is an ongoing and institutionalized process that has become part of daily operations. While it is supported by training, supervision, and organizational culture, its effectiveness is hindered by human error, resource limitations, operational pressures, and technological risks. Thus, implementation requires continuous improvement and adaptive strategies to ensure consistent protection of clients' personal data.

Informants conceptualize data privacy as an essential legal, ethical, and professional obligation embedded within their institutional mandate. It is not viewed as a separate function but as an integral component of security operations and service delivery. Therefore, effective data privacy practice depends on balancing operational efficiency with strict adherence to confidentiality, accountability, and lawful data handling.

The implementation of data privacy policies is shaped by a combination of internal and external factors. Internal factors such as leadership, training, policy clarity, organizational culture, resources, and monitoring systems interact with external pressures such as laws, client expectations, technological developments, cybersecurity threats, and public scrutiny. Hence, effective compliance is determined by the alignment and strength of both organizational capacity and environmental conditions.

Data privacy practices significantly influence clients' trust in security agencies. Proper handling of personal data enhances credibility, professionalism, and long-term trust, while mishandling or data breaches undermine confidence, damage reputation, and reduce client cooperation. Therefore, trust is a direct outcome of consistent and responsible data privacy practices.

Recommendations

1. **Strengthen data privacy governance through comprehensive policies, leadership commitment, and legal compliance.** Private security agencies should institutionalize a comprehensive Data Privacy Governance Policy that clearly defines roles, responsibilities, and standard operating procedures. Agency leadership should demonstrate strong commitment by promoting accountability, regularly reviewing policies, ensuring compliance with the Data Privacy Act of 2012 and National Privacy Commission guidelines, and updating organizational practices to address emerging legal, operational, and technological developments.

2. Enhance personnel competency and foster a culture of data privacy and ethical responsibility. Agencies should implement continuous capacity-building programs through regular, practical, and scenario-based data privacy training. At the same time, management should cultivate an organizational culture that recognizes data privacy as a shared responsibility grounded in professionalism, confidentiality, ethical conduct, and public service integrity, thereby reducing human errors and strengthening employee accountability.

3. Improve operational systems, technological safeguards, and resource support. Agencies should invest in secure information systems, including encrypted databases, access control technologies, cybersecurity measures, and monitoring tools to protect personal information. Adequate staffing, financial resources, and logistical support should likewise be provided to ensure that operational demands do not compromise the proper implementation of data privacy measures.

4. Institutionalize monitoring, auditing, transparency, and continuous improvement. Regular compliance audits, data access monitoring, incident reporting mechanisms, and performance evaluations should be institutionalized to identify gaps and strengthen implementation. Agencies should also maintain transparency by clearly communicating their data privacy practices to clients, thereby enhancing public trust while ensuring that operational efficiency is consistently balanced with the principles of necessity, proportionality, confidentiality, and authorized access.

5. Future researchers may conduct similar studies in other security agencies or related organizations using different research designs or larger populations to validate, compare, and expand the present findings. Future studies may also examine the effectiveness of the proposed Data Privacy Governance Policy after its implementation to determine its impact on organizational compliance, employee behavior, and client trust.

6. Adopt the proposed Data Privacy Governance Policy.

Acknowledgement

The researcher expresses his profound gratitude to the individuals whose guidance, support, and cooperation contributed significantly to the successful completion of this dissertation.

First and foremost, the researcher extends his sincerest appreciation to **DR. MARLYN P. WACNAG,** *Dissertation Adviser*, whose scholarly expertise, philosophical insight, and steadfast guidance provided direction, clarity, and intellectual depth throughout the conduct of this study. Her constructive criticisms, professional encouragement, and unwavering commitment to academic excellence greatly strengthened the conceptual, methodological, and ethical foundations of this research.

Likewise, deepest appreciation is conveyed to **ATTY. JOAQUIN R. ALVA, PhD**, *Dean of the Graduate School*, for his invaluable leadership, academic rigor, and guidance in fostering a culture of scholarship and research excellence. His support and dedication to graduate education significantly contributed to the completion of this academic undertaking.

Further, he expresses his sincere gratitude to the distinguished members of the *Panel of Examiners* for their invaluable time, scholarly insights, and professional recommendations, which greatly enriched this dissertation. Special recognition is accorded to the participants and key informants from the security agencies in *Region IV-A (CALABARZON)*, whose cooperation, honesty, and willingness to share their experiences, insights, and perspectives on *data privacy* and *governance* made this study possible. Their participation served as the empirical foundation of this dissertation and contributed immensely to the realization of its objectives.

Heartfelt thanks are likewise extended to the researcher's colleagues, peers, and friends, whose encouragement, intellectual exchanges, and moral support

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

became constant sources of inspiration during the most demanding phases of this academic undertaking.

The researcher is especially indebted to his family and relatives for their unwavering love, patience, understanding, and support. Their sacrifices, prayers, and encouragement provided the strength, perseverance, and motivation needed to complete this doctoral work.

Above all, the researcher humbly and faithfully thanks *God Almighty* for His wisdom, strength, guidance, and countless blessings bestowed throughout this academic journey. Without His grace, this achievement would not have been possible.

This work is respectfully offered in the spirit of advancing *ethical governance*, protecting *individual rights*, and contributing to the continuing philosophical and scholarly discourse on *data privacy* within the context of public safety and security.

REFERENCES

1. *Afzal, M., & Panagiotopoulos, P. (2025). Data in policing: An integrative review. International Journal of Public Administration, 48(7), 411–430.*
2. *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, 2215–2224.*
3. *Andaya, E. J., Orlina, R. J. G., & Illustre, R. G. (2025). Digital governance in the Philippines: A scoping review of current challenges and opportunities. Global Sustainability Research, 4(1).*
4. *Ayuyang, D. M., & Ayuyang, R. R. (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), 1074–1086.*
5. *Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. The British Journal of Criminology, 60(6), 1502–1522.*
6. *Bennett, C. J., & Raab, C. D. (2020). The governance of privacy: Policy instruments in global perspective (2nd ed.). MIT Press.*
7. *Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa*
8. *Camorongan, J. R. C. (2023). The pledge of smart city development: The e-governance (under) development in the Philippines. IOER International Multidisciplinary Research Journal, 5(3), 1–14. https://doi.org/10.54476/ioer-imrj/042507*
9. *Casaburo, D., & Marsh, I. (2024). Ensuring fundamental rights compliance and trustworthiness of law enforcement AI systems: The ALIGNER Fundamental Rights Impact Assessment. AI and Ethics.*
10. *Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.*
11. *Dasgupta, S., Kumar, R., & Sharma, P. (2025). Mitigating organizational risk through privacy preservation and ethical data governance. Journal of Risk Analysis and Crisis Management, 19(2), 142–159.*
12. *Dasgupta, R., Mekala, S. H., Jaigirdar, F. T., Anwar, A., & Chang, L. (2025). Unlocking Australia'sAI usage in law enforcement from human involvement perspective: A systematic literature review. AI & Society.*
13. *Dausan, A. F., Fabro, J. G. M., Reyes, S. M., Fabro, A. B., Gelacio, R. Q., Reyes, G. A., Train, C. G., & Tanigue, Y. (2025). Securing public trust through blockchain integration: The case of the National Police Clearance System in the Philippines. International Journal of Multidisciplinary: Applied Business and Education Research, 6(9).*
14. *Dela Rosa, A. P. M. (2025). Assessing data privacy attitudes of Information Technology students: Basis for awareness enhancement. International Journal of Multidisciplinary: Applied Business and Education Research, 6(10).*
15. *Donatz-Fest, I. (2024). The 'doings' behind data: An ethnography of police data construction. Big Data & Society, 11(3).*
16. *Espiel, A. M. G. (2024). E-government implementation in Calamba Water District and public trust: Basis for enhancement program. Journal of Interdisciplinary Perspectives, 2(7).*
17. *European Data Protection Board. (2026). Guidelines 1/2026 on processing personal data, accountability, and risk reduction mechanisms. EDPB Register of Decisions and Guidelines.*
18. *European Union Agency for Fundamental Rights. (2022). Facial recognition technology: Fundamental rights considerations in law enforcement.*
19. *Floridi, L. (2020). The logic of information: A theory of philosophy as conceptual design. Oxford University Press.*
20. *Galang, G. M. B., & Villa-Buena, E. S. (2024). Philippine Social Security System: An evaluation of strategic approach to digital services. International Journal of Multidisciplinary: Applied Business and Education Research, 5(8).*
21. *Gstrein, O. J., & Beaulieu, A. (2022). Technological sovereignty, artificial intelligence, and the governance of data. Regulation & Governance, 16(3), 670–689.*
22. *Guazzo, G. M., Rosati, P., Troisi, O., & Lynn, T. (2026). Balancing privacy and trust: Social acceptance of video-based traffic sensors in smart city initiatives. Government Information Quarterly, 43(1), 102099.*
23. *Guler, A. (2025). Perceived fairness and privacy assurance in organization-client trust models. Journal of Cybersecurity and Data Governance, 18(1), 45–62.*
24. *Guler, A., Kula, S., & Boke, K. (2025). Examining public support for AI in policing: The role of perceived procedural justice. Police Practice and Research, 26(6), 673–695.*
25. *Herrewijnen, E., Loerakker, M. B., Vredenborg, M., & Woźniak, P. W. (2024). Requirements and attitudes towards explainable AI in law enforcement. In DIS '24: Proceedings of the 2024 ACM Designing Interactive Systems Conference.*
26. *Information Commissioner's Office. (2025). Personal data breach management and reporting of police forces in England and Wales: Outcomes report.*
27. *Jones, A. M., Vance, A., & Jenkins, J. L. (2024). Protecting organizational reputation: The impact of transparent data privacy practices on client confidence. Information Systems Research, 35(4), 1120–1138.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

28. *Kiram, D. A. K., Kiram, M. M., Hadjibun, J.-A. A., & Taraji, M. (2024). Data governance and privacy in Sulu, Philippines: Building trust and ensuring accountability in digital public service delivery. Open Access Indonesia Journal of Social Sciences, 8(1), 1952–1966.*
29. *Li, B. (2024). Responsible data handling and user cooperation: The mediating role of client trust. Information & Management, 61(3), Article 103890.*
30. *Li, W., Li, Z., Zhang, Y., & Li, A. (2025). Mapping empirical research on GDPR effectiveness: A systematic review. Computer Law & Security Review, 54, 105789.*
31. *Lyon, D. (2022). Pandemic surveillance. Polity Press.*
32. *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 and manual for good governance. Edelweiss Applied Science and Technology, 9(1), 302–315.*
33. *Moustakas, C. (1994). Phenomenological research methods. SAGE Publications.*
34. *National Privacy Commission. (2016). Implementing rules and regulations of the Data Privacy Act of 2012. National Privacy Commission.*
35. *National Privacy Commission. (2020). NPC annual report 2020. https://www.privacy.gov.ph*
36. *National Privacy Commission. (2022). NPC annual report 2022. https://www.privacy.gov.ph*
37. *National Privacy Commission. (2022a). NPC Circular No. 2022-01: Guidelines on administrative fines.*
38. *National Privacy Commission. (2022b). NPC Circular No. 2022-04: Registration of personal data processing system, notification regarding automated decision-making or profiling, designation of data protection officer, and National Privacy Commission Seal of Registration.*
39. *National Privacy Commission. (2023). NPC annual report 2023. https://www.privacy.gov.ph*
40. *National Privacy Commission. (2023a). NPC launches online registration system for data processing systems.*
41. *National Privacy Commission. (2023b). Advisory Opinion No. 2023-025: Multi Face ID initiative for fraud prevention.*
42. *National Privacy Commission. (2023c). NPC Circular No. 2023-06: Security of personal data in the government and the private sector.*
43. *National Privacy Commission. (2024a). NPC commends new DILG issuance enhancing data privacy compliance among LGUs.*
44. *National Privacy Commission. (2024b). Reminder on sharing photos and videos containing personal data.*
45. *National Privacy Commission. (2024c). NPC Circular No. 2024-02: CCTV systems.*
46. *National Privacy Commission. (2025a). NPC Advisory No. 2025-01: Clarification on certain provisions of NPC Circular No. 2020-03 on data sharing agreements.*
47. *National Privacy Commission. (2025b). NPC Advisory No. 2025-02: Guidelines on privacy engineering in systems life cycle processes.*
48. *Nieuwenhuizen, E. N., Meijer, A. J., Bex, F. J., & Grimmelikhuijsen, S. G. (2024). Explanations increase citizen trust in police algorithmic recommender systems: Findings from two experimental tests. Public Performance & Management Review. Advance online*
49. *publication. https://doi.org/10.1080/15309576.2024.2443140.*
50. *Nieuwenhuizen, R., van der Meer, S., & De Vries, J. (2025). Accountability and institutional trust in digital security services. Security Journal, 38(2), 210–228.*
51. *Obendiek, A. S. (2025). Data governance and emerging technological risks in public administration. Information Polity, 30(1), 45–61.*
52. *Organisation for Economic Co-operation and Development. (2022). OECD digital security risk management framework.*
53. *Republic Act No. 10173. (2012). Data Privacy Act of 2012. Republic of the Philippines.*
54. *Republic Act No. 11917. (2022). Private Security Services Industry Act. Republic of the Philippines.*
55. *Rössler, B. (2021). The value of privacy. Polity Press.*
56. *Sagana, M. (2025). Operationalizing privacy: Aligning service delivery with data ethics in client relations. International Journal of Information Management, 75, Article 102712.*
57. *Sancon, R. J. S. (2023). Data privacy best practices of a local higher educational institution: A model for governance. IOER International Multidisciplinary Research Journal, Special Issue, 9–16.*
58. *Spyropoulos, A. Z., & Tsiantos, V. (2025). Interoperable semantic systems in public administration: AI-driven data mining from law-enforcement reports. Computers, 14(9), Article 376.*
59. *Sunde, I. M. (2023). To have or have not: Limiting the data available for subsequent use by the police. New Journal of European Criminal Law, 14(4), 495–511. https://doi.org/10.1177/20322844231214486*
60. *Stahl, B. C. (2022). Artificial intelligence, ethics, and governance: A critical review. AI & Society, 37(1), 1–16.*
61. *Tano, I. M. (2024). Digitalization in local governance. Pantao (International Journal of the Humanities and Social Sciences), 3(3).*
62. *Zuboff, S. (2020). The age of surveillance capitalism. PublicAffairs.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 8| August 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Interview Guide

1. How do informants describe their experiences in implementing data privacy policies when handling clients' personal data?

1.1 Can you describe your experiences in implementing *data privacy policies* when handling *clients' personal data* in your agency?

1.2 What procedures or practices do you usually follow to protect *clients' personal information* in the course of your work?

1.3 What challenges or difficulties have you encountered in applying *data privacy policies* in actual practice?

2. How do informants within security agencies conceptualize data privacy in relation to their institutional mandates and the handling of clients' personal data?

2.1 How do you understand or define *data privacy* in the context of your work in a *security agency*?

2.2 How do you relate *data privacy* to the mandate, duties, or responsibilities of your agency?

2.3 In your view, how should a *security agency* balance its operational functions with the protection of *clients' personal data*?

3. What factors influence the implementation of data privacy policies concerning clients' personal data within security agencies?

3.1 What internal factors within your agency influence the implementation of *data privacy policies*?

3.2 What external factors, such as laws, clients, or technology, affect the way your agency implements *data privacy practices*?

3.3 In your opinion, what factors most strengthen or weaken compliance with *data privacy policies* in your agency?

4. How do data privacy practices in the handling of clients' personal data shape clients' perceptions of trust toward security agencies?

4.1 Based on your observation, how do *data privacy practices* affect clients' trust in your agency?

4.2 In what ways does proper handling of *clients' personal data* help build confidence and credibility among clients?

4.3 What happens to clients' perceptions of the agency when *personal data* are mishandled, exposed, or inadequately protected?

5. What policy framework may be proposed based on the findings of the study?