ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

Application of Privacy Engineering Techniques in Software Development for the National Privacy Commission

Measuring Effectivity baased on the Deployment of the Data Breach Notification Management System

Conrad D. Dela Cruz
Professional Science Master in Cyber Security
Holy Angel University, Angeles city, Philippines

Abstract:- The study investigated the implementation of privacy engineering in software development at the National Privacy Commission (NPC) with a specific focus on the Data Breach Notification Management System (DBNMS). Objectives include identifying the factors that contribute to the success or failure of privacy engineering in the NPC's software development context, to provide valuable insights into the integration of privacy measures. This includes the development of actionable guidance for the effective integration of privacy and security in software engineering at the NPC, tailored specifically for NPC engineers and encompassing methodologies for incorporating privacy engineering throughout the software development life cycle. This is to empower NPC software engineers with practical tools and strategies to create a secure and privacy-respecting environment. Qualitative methodology and thematic analysis approach were utilized to assess the effectiveness of privacy engineering techniques. To gather insights, semi structured interviews were conducted with both internal and external stakeholders composed of software developers, data protection officers, and other internal and external users of the DBNMS. Evaluation yielded positive remarks both from internal and external participants. Factors that contributed to the success and failure of privacy engineering techniques in software development include rapid evolution of technology, lack of funds, and stakeholder engagement, among others. Overall, the findings are expected to contribute to the broader discourse on privacy engineering and have implications for policymakers, software development practitioners, and organizations looking to enhance their privacy practices in the digital age.

Keywords:- *Privacy Engineering, Privacy Integration in Software Development.*

I. INTRODUCTION

Privacy has become a critical issue for both software developers and end users. With the increasing amount of personal data and sensitive personal data processed, collected, and shared by software applications, the need for privacy-conscious software practices has become more urgent than ever.

One of the main privacy problems with current software development practices is the neglect of privacy throughout the software life cycle. Many developers prioritize functionality, performance, and user experience over privacy. Therefore, privacy controls and safeguards are often added after the fact, if at all. This can lead to personal data breaches which in turn will result in legal liabilities for organizations.

According to a report from the US Government Accountability Office about the data breach of Equifax on 2017, 143 million US consumers had been affected by the breach that is caused by a vulnerability on a web framework that the software developers used in its publicly facing portal (Marinos & Clements, 2018). The incident required the company to pay 700 million US dollars to settle federal and state investigations (Leonhardt, 2019).

In 2018, Marriott International experienced a data breach that exposed the personal information of 500 million customers. The breach was caused by a vulnerability in a third-party software application used by Marriott's Starwood brand, which allowed hackers to gain access to sensitive data (Gosh, 2023).

The above-mentioned personal data breaches are just a few examples of high impact breaches caused by poor software development practices. It is important to note that incidents such as these are still on the rise. In this regard, the different organizations recognized the need to adopt security and privacy-preserving techniques in software development. The National Privacy Commission is seeking to continuously improve the privacy and security posture of its software systems and one of the methods is the adoption of Privacy

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

Engineering techniques in the development of the Commission's software applications.

This paper aims to assess the effectiveness of applying privacy engineering practices throughout software development, particularly with the Data Breach Notification Management System (DBNMS). The DBNMS is an online platform developed by NPC that enables organizations to report data breaches and Annual Security Incident Reports to the Commission and manage the notification process. Privacy engineering techniques were applied during the initial phases of development, implemented during deployment, and are still being monitored to ensure its privacy and security stature, as recommended by privacy engineering methodologies.

The DBNMS is developed following the agile methodology. Agile Software Development is a software development methodology that values flexibility, collaboration, and customer satisfaction. It is based on the Agile Manifesto, a set of principles for software development that prioritize individuals and interactions, working software, customer collaboration, and responding to change (Naidu, 2023). According to an article, Feature-driven development (FDD) is a development methodology that emphasizes the delivery of small, incremental features or units of functionality as the primary means of progress. It is an agile approach that is designed to be flexible and responsive to changing requirements and priorities (Stanke, 2022). The development of the DBNMS can be summarized into 2 phases; The Planning Phase and the Construction Phase and each of these phases are also divided into smaller activities or stages.

The scope of this paper is limited only to the assessment of the efficacy of the application of privacy engineering techniques applied during the development of the DBNMS. This study aims to achieve the following:

- Evaluation of the effectiveness of the application of privacy engineering techniques in software development.
- Identification of factors that contribute to the success or failure of privacy engineering techniques in software development at the NPC.
- Development of a software development guide with the methodologies on how to integrate privacy engineering into the software development life cycle for NPC engineers. This template, modified in MS Word 2007 and saved as a "Word 97-2003 Document" for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

II. REVIEW OF RELATED LITREATURE

Privacy has become a critical concern in the digital era, where large amounts of personal data and sensitive personal data are collected, stored, and analyzed by various entities. Privacy engineering aims to provide solutions to address privacy concerns in the design and development of software systems. The proponent reviewed studies related to the topic and are presented in this section. This literature review examines the various studies and literature relating to the application of privacy engineering in software engineering following the Needs, Solutions, Differentiation and Benefits Framework (NSDB).

The benefits of using software for a variety of services are becoming essential in today's daily lives. However, poor software development practices lead to compromise of not only personal data but sensitive personal data as well. Organizations lose huge amounts of money in legal liabilities because of data breaches. Implementing security techniques after the software development lifecycle is not enough to prevent or minimize the possibility of personal data breaches. According to a recent report, the cost of poor software quality in the US is estimated to have grown to at least $2.41 trillion. Cybercrime losses due to existing software vulnerabilities increased significantly, with losses rising by 64% from 2020 to 2021. Those losses have not yet been determined for 2022 (Consortium for Information and Software Quality, 2022). This predicament has brought about the development of techniques in applying security throughout the software development lifecycle. One of which is privacy engineering methodologies that can be applied to a variety of processes and applications, but most importantly within the software development space.

The evolution of privacy regulations has also made consumers more sensitive and more aware of their privacy rights. According to an article by Sean Falconer, the days are long gone when users did not think about the information they give away freely to companies and applications. For example, in the April 2021 iOS 14.5 update, 96% of iPhone users opted out of having their location tracked across apps (Falconer, 2022). Organizations may face legal problems if these privacy rights are not respected. This, in effect, transforms the way organizations provide their services, especially those that are software based.

However, challenges in applying privacy and security in software development are also common. According to a paper review by Nurgalieva, Frik and Doherty, many studies recognize the difficulty for developers to translate privacy and security requirements into specific software development processes (Nurgalieva et al., 2021). The same paper also states that the lack of incentives for software developers can impact their privacy and security practices, potentially encouraging them to prioritize functionality over security and privacy. This

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

is supported by a similar study by Sousa, Caneda and Silva, where their research results showed that most respondents were aware of the Brazilian data privacy law (Lei Geral de Proteção de Dados or LGPD) guidelines, but lacked specific implementation techniques, with accountability being the most challenging principle (Rocha et al., 2023). This highlights the gap between data privacy knowledge and actual implementation of privacy requirements among software developers.

The lack of integration of data privacy in software development is also echoed in a statement from an article, emphasizing that in modern product development, software engineers follow a virtuous cycle where they plan, design, make sure code is well tested, and scale up the implementation. These are all part of a continuous process that defines the product's life cycle. However, data privacy is generally not part of this process. Features are planned, designed, and implemented long before thinking about the privacy implications (Falconer, 2022).

According to a journal written by Tahaei, et al. 2023, another issue identified with integrating privacy in software development is that developers who don't actively consider privacy issues may find it challenging to address them due to the lack of prompts or reminders in their development toolbox. This invisibility of privacy within their workflow further complicates the integration of privacy features into software projects (Tahaei et al., 2023). In the same journal, the researchers also mentioned an issue in education. A computer science curriculum typically focuses on software development, mathematics, and algorithms, with less emphasis placed on ethics and privacy. This focus trains software developers who are competent in developing functional software but may pay less attention to building privacy-preserving systems (Tahaei et al., 2023).

Privacy and security can be integrated into the software development lifecycle to ensure that personal information and sensitive personal information processed by the software system in the future are mitigated from data breaches, although not entirely prevented. While other layers like organizational, physical, and other technical security measures need to be considered for comprehensive privacy and security, having a secure and privacy-designed system will nevertheless lessen the burden on organizations and data subjects in the event of a malicious attack.

In addition, integrating security measures into a system does not guarantee the prevention of all privacy problems. The National Institute for Standards and Technology (NIST) provides two (2) examples where security measures can cause privacy concerns. According to a NIST publication, there are security issues unrelated to privacy, just as there are privacy issues unrelated to security. For example, in the energy sector, some communities have responded negatively to smart meters due largely to concerns that the collected information can reveal in-home behavior, with less focus on concerns about the utilities' ability to keep the information secure. Even actions taken to protect Personally Identifiable Information (PII) can have privacy implications. For example, security tools like persistent activity monitoring can raise concerns about the extent to which information unrelated to cybersecurity purposes is revealed about individuals (NIST, 2017).

A Software Development Life Cycle (SDLC) outlines each stage of software development, breaking down the process into distinct phases (Velimirovic, 2022). The exact number and nature of steps depend on the business and its product goals. On average, most companies define SDLCs with five to seven phases, although more complex projects may reach ten or more stages. The most common phases include:

- Planning – This is the requirements analysis stage where the overview of the project is discussed, what is the purpose of the software project and its objectives as well as the requirements. Privacy engineering can be integrated in this stage by following best practices in data privacy such as data minimization and following the principle of proportionality,
- Coding – This is the actual development phase, privacy engineering can be used to ensure privacy protections are in place in the software, encryption, code obfuscation, anonymization or pseudonymizations of personal data and sensitive personal data can be used at this stage.
- Testing – This is the stage wherein the software is tested for its functionality. In this process, security and privacy can also be tested.
- Deploy – Prior to deployment, a Privacy Impact Assessment should be conducted to ensure that all possible privacy risks are identified and can be mitigated.
- Maintenance - Software systems should be protected after it was deployed, by using firewalls and other security monitoring tools as well as anti DDOS tools at this stage, management and end users alike may ask for a change or ask for an additional feature on the system, this should also undergo careful planning, PIA and determination of privacy risks and controls.

This is not an exhaustive list of the privacy engineering methodologies that can be applied to the SDLC, nor are these the complete stages of an SDLC. However, the list above may be used as a reference if one would like to embed privacy engineering into their software systems during its development.

Because of growing concerns about personal data breaches, privacy regulations impose increased accountability on software developers to ensure their products comply with the regulations. This may involve implementing specific security measures, obtaining user consent, and providing transparency about data usage. One solution is to integrate privacy into the design stage of a process or a system. Under the GDPR, a key obligation is the implementation of Privacy by Design and Default in the early stages of product development. Failing to address privacy at this stage may lead to hefty fines and legal problems (Agarwal, 2022).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

According to a journal by Campanille, et al. 2022, a methodological effort is required to systematically integrate privacy regulations into software development. The paper also emphasizes the need to align software development lifecycles with privacy regulations to ensure better compliance (Campanile et al., 2022).

Privacy by Design (PbD) is a proactive measure that aims to embed the concept of privacy in all data-processing activities right from the outset. Thus, it is not a reactive measure or countermeasure taken in response to a breach. PbD takes a design thinking approach to managing individual control over personal data flow, incorporating it into systems and technologies by default (PWC, 2021). It is believed that Privacy by Design (PbD) is an important tool to protect privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures (Bernsmed, 2016).

According to a study conducted by Andrade et al. 2023, implementing Privacy by Design (PbD) throughout the software development lifecycle (SDLC) faces challenges due to a lack of supporting elements. The systematic literature review revealed a scarcity of models, processes, and tools specifically designed to support PbD across the entire SDLC. This deficiency makes it difficult to effectively integrate privacy considerations from the early stages of system development (Andrade et al., 2023).

Aside from the Privacy by Design methodology, various strategies and standards are developed in order to ensure the security of software products. One notable example is the DevOpsSec (Development, IT Operations and Security) approach. It is the combination of three terms -- development, security, and operations. It is the adoption of security from the beginning of a software or application development lifecycle and is developed to address the old practice of adding security to an application later in the lifecycle, after the development phase. The advancement of cloud platforms, microservices, and containers created a bottleneck to the traditional development approach. Security was unable to keep up with the rapid releases as developers adopted agile and DevOps practices for modern application development and deployment (Javed, 2022). It is expected that software applications developed using this approach will save the organization from legal issues caused by breaches.

The latest approach in the privacy landscape is Privacy Engineering. This emerging field develops tools, methodologies, and processes to help meet the privacy requirements and expectations of regulators and customers. Privacy engineering integrates privacy considerations with technologies and techniques for data protection and cybersecurity (Williams, 2022).

While the DevSecOPs framework addresses software security concerns by integrating security practices into the Software Development Lifecycle, it doesn't guarantee complete protection from privacy-related legal issues. It should be noted that security does not equate to privacy. Privacy focuses on protecting personal information and giving individuals control over their data, while security focuses on protecting data from unauthorized access and ensuring its integrity and confidentiality. Both privacy and security are important aspects of data protection and are often addressed together in software development and other areas of technology. However, it is important to note that one cannot have privacy without security, hence, the relationship between these two concepts.

Although Privacy by design and Privacy engineering share the same goal of data protection and empowering consumers or data subjects with control over their personal data, they differ in their approach. Privacy by design focuses on translating privacy requirements into an actionable implementation plan. Privacy engineering, on the other hand, bridges the gap by providing the technical know-how to execute that plan. As Cavoukian et al. (2014) stated, Privacy by Design provides the "what," while privacy engineering provides the "how."

While PbD approach offers guidelines for integrating privacy considerations into systems, it often faces criticism for its lack of practical guidance. In an article by Spiekermann-Hoff (2012), challenges of implementing PbD are enumerated, including how to get management buy-in for an organization's privacy strategy. The article highlights how management often avoids invovlement in crafting privacy strategies, leaving privacy issues to be addressed by lawyers.

There is a significant shift in focus towards the specific actions needed to achieve the outcomes promised by the Privacy by Design framework. This has fueled the growth of privacy engineering, the technical counterpart to the policy roles of the Chief Privacy Officer (CPO) and the Data Protection Officer (DPO) (Williams and Nee, 2022). The same paper states that Privacy engineering, grounded in a comprehensive understanding of privacy concepts and design principles, offers a structured approach to compliance. Moreover, thoughtful deployment of privacy engineering enables a flexible and adaptable approach to meeting future regulatory or customer requirements. As Sampath (2022) emphasizes, these limitations of PbD can be mitigated when used in conjunction with privacy engineering methodologies. Sampath argues that privacy engineering operationalizes the Privacy by Design framework by providing methods, tools, and metrics to develop systems that protect privacy.

While data processing systems all require a privacy notice, statement, or policy, these documents alone are insufficient to ensure the protection of personal and sensitive personal information. According to a blog by Claire Park (2020), notice and consent, which require private entities to notify individuals and obtain their permission before collecting and using their personal data, are inadequate for both informing individuals and protecting their privacy.

A research study by Tahaei et al. (2023) identifies a key challenge in implementing privacy requirements during software development: multi-stakeholder engagement. Integrating privacy features effectively necessitates the involvement of various stakeholders, such as organizations,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

educators, and regulators. Coordinating and aligning the efforts of these different parties can be a complex and time-consuming process for developers.

Another study by Sangaroonsilp et al. (2022) reinforces this notion. To ensure privacy compliance and security in software systems, the study recommends collaboration between organizations or software developers with privacy experts and legal professionals. This collaboration helps mitigate privacy vulnerabilities by ensuring software applications comply with privacy regulations and industry standards. The study also emphasizes the importance of regular privacy assessments and audits of software applications. These assessments help identify and address potential privacy weaknesses before they can be exploited.

Applying privacy engineering in software development is essential for protecting user privacy, complying with regulations, building trust with users, and creating a competitive advantage. By incorporating privacy principles and practices into the software development process, organizations can create products that respect users' privacy. NIST 8062 emphasizes this point, stating that privacy engineering, based on systems engineering principles, can help ensure appropriate privacy principles are applied throughout an agency's system life cycle to achieve stakeholder objectives for protecting individual privacy. Additionally, privacy engineering can provide a strong evidence base to support claims that the desired level of trustworthiness has been achieved (NIST, 2017).

Privacy engineering techniques aim to embed privacy requirements and considerations into software development processes to ensure the protection of personal information and mitigate privacy risks. However, applying these techniques in practice faces challenges. The lack of standardized methods, tools, and awareness among software engineers hinders widespread adoption. In addition, as a relatively new concept, privacy engineering requires further research to establish concrete guidelines and best practices for integration into software development, particularly within the Philippines.

The importance of privacy engineering is highlighted in a blog by Dulberg (2021). It states that there isn't a single 'right' way to implement privacy by design. However, an array of emerging best practices, known as "privacy engineering," helps those who want to build products, systems, and processes that integrate privacy and trust without compromising innovation. This notion is echoed in a study by Martin and Kung (2018). Their study shows that Privacy Engineering integrates privacy considerations into software and systems engineering methods, ensuring that privacy is a fundamental aspect of the design and development process. This approach helps create products that prioritize data protection and privacy.

One objective of this study is to develop a software development guide for National Privacy Commission (NPC) engineers. This guide will help them develop software projects that are not only compliant with the Data Privacy Act of 2012, its Implementing Rules and Regulations, and issuances of the Commission, but are also privacy-centric and secure for future projects. A similar tool was created in a study by Rocha et al. (2023). Their research paper proposes a reference guide to assist ICT professionals in understanding and implementing the principles of Brazil's Data Privacy Law (LGPD).

A guide for software developers is also a proposed solution stated in a research paper. According to the paper, regulators at the top of the chain may not intend to engage with the details of tool building and instead provide high-level guides about privacy (e.g., CCPA and GDPR). However, translation of these guides to technical requirements is often left to organizations and developers One approach to bridge the gap between these parties is to fund independent academic research groups or not-for-profits to build tangible and understandable guides for the developer community (Tahaei et al., 2023).

In conclusion, although privacy engineering techniques have the potential to enhance the privacy and security of software systems, their effective implementation requires standardized methods and tools, collaboration between privacy and software development teams, and increased awareness and expertise among software engineers as well as concrete guidelines from regulators.

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the file "MSW_USltr_format".

III. CONCEPTUAL FRAMEWORK

The conceptual framework in this study utilized the Input Process Output (IPO) method in visualizing the output of the study as presented in Figure 1. The proponent used the Software Development Models, Privacy by Design Techniques, Software Engineering Practices, and Privacy Engineering methodologies. Data breach reports based on the collected references from the reviewed related literature and findings from the semi-structured interview were also used as inputs. The process involved the evaluation of findings and data analysis. Finally, the study's output was the development of an internal software development guideline for the NPC and an assessment report on the effectiveness of the applied privacy engineering techniques in software development in the DBNMS.

A. Objectives of the Study

➢ *The following are the Objectives of the Study:*

- To evaluate the effectiveness of the application of privacy engineering techniques in software development.
- To identify the factors that contribute to the success or failure of privacy engineering techniques in software development at the NPC.
- To provide guidance on how to effectively integrate privacy and security in software engineering within the National Privacy Commission based on the conclusion

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

that will be presented in this study. A software development guide with the methodologies on how to integrate privacy engineering to the software development life cycle will be developed to be used by NPC engineers.

B. Scope and Delimitations

This study aimed to determine the effectiveness of privacy engineering techniques in software development. The study focused on the implementation and application of privacy engineering in software engineering, particularly in the development of the Data Breach Notification Management System (DBNMS).

The study was limited to the application of privacy engineering techniques in the development of the DBNMS and did not include other systems within the NPC. It was also conducted within a limited timeframe, specifically two (2) to three (3) months.

C. Significance of the Study

The study on the application of privacy engineering techniques in software development and its effectivity in preventing and managing data breaches through the deployment of the Data Breach Notification Management System (DBNMS) in the National Privacy Commission (NPC) in the Philippines is significant for the following reasons:

- Advancement of knowledge not only to privacy professionals but also to software developers and security professionals: The study will contribute to the advancement of knowledge on the effectiveness of privacy engineering techniques in software development in the context of the NPC. It will provide insights into the factors that contribute to the success or failure of privacy engineering techniques in the prevention or mitigation of security incidents including personal data breaches by developing a more secure and privacy focused software or application.
- Improvement of privacy engineering practices not only for the software developers of NPC but also for the organization's security team, compliance and possibly also for external stakeholders including personal information controllers and personal information processors: The study will help identify the strengths and weaknesses of privacy engineering practices that are applied or integrated in software development based on its implementation in the DBNMS. The study's findings can provide recommendations for improving privacy engineering practices particularly in software development.
- Protection of personal data: The study is important in ensuring the protection of personal data. Insecure software may lead to personal data breaches which can lead to the exposure of personal information and even sensitive personal information, this can have profound consequences for individuals. The study's findings can help develop more secure and privacy-focused software and help mitigate if not prevent personal data breaches, thereby protecting the privacy and security of personal data.
- Compliance with regulations: The study will be able to provide another way for organizations on how they will be able to comply with the Data Privacy Act of 2012, its IRR and the issuances of the NPC, the study aims to provide guidance on how to develop a more secure and privacy focused software using or following the implementation of privacy engineering techniques that were used in the development of the DBNMS.
- Contribution to public policy: The study can contribute to the development of public policy on data privacy and security, specifically in the development of secure and privacy focused software. The study's findings can be used as a basis for developing a guide on how to implement or integrate privacy engineering techniques in software development.

"Magnetization (A (m(1)," not just "A/m." Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)," not "Temperature/K."

IV. METHOD

This section outlines the research methodology that was used to investigate the application of privacy engineering techniques in software development at the National Privacy Commission (NPC) and to measure its effectiveness based on the development and the implementation of the Data Breach Notification Management System.

A. Philosophical Underpinning

The researcher follows the interpretivism approach or more commonly known as naturalist approach to research (King et al., 2019). The naturalist approach advocates understanding phenomena in their natural context and complexity and aligns with the objectives of this study which seek to evaluate the effectiveness of privacy engineering techniques in software development, identify contributing factors to their success or failure, and provide guidance on integrating privacy and security in software engineering within the National Privacy Commission (NPC). The data collection involved conducting semi structured interviews. According to King et al, the focus for research might be to uncover how people feel about the world and make sense of their lives from their vantage points. Therefore, qualitative interviewing fits; conversing with people enables them to share their experiences and understandings.

The researcher believes that the diverse backgrounds and experiences of the participants, even though the number is minimal, will provide useful insights for the study. Interpretivism perceives experience and understanding as seldom straightforward. People navigate complex realities, often attaching different interpretations and meanings to seemingly similar 'facts' and events (King et al., 2019).

The philosophical underpinning of this research underscores a commitment to understanding privacy preservation in systems within its natural context, embracing complexity, diversity, and reflexivity. By adopting a naturalist approach, the researcher aims to generate insights that are grounded in empirical observations and situated within real-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

world contexts, contributing to a deeper understanding of privacy preservation practices and informing the development of more effective strategies for protecting privacy in systems.

B. Research Design

This study employed a descriptive research design with a qualitative approach. Semi-structured interviews were chosen as the primary method for data collection. A questionnaire was also carefully crafted and prepared for selected participants. This approach aimed to explore the effectiveness of privacy engineering techniques in software development at the National Privacy Commission (NPC) through the development of the Data Breach Notification Management System (DBNMS). The qualitative methods provided an in-depth understanding of the topic through interviews and the questionnaire.

C. Data Collection

This section describes all the details of the data gathering tools, instruments, and techniques used in the research design. Data collection relied on interviews conducted in accordance with Republic Act 10173 or the Data Privacy Act of 2012, its implementing rules and regulations, and the issuances of the National Privacy Commission. For online interviews, an online platform was used, with internet usage expenses not covered by the researcher unless specifically requested by the participant.

A semi-structured interview served as the primary method for data collection. Semi-structured interviews involve asking questions within a predetermined thematic framework (George, 2022). The interviews were conducted through teleconferencing using an online meeting platform. A recent study by Irani (2019) highlights the advantages of videoconferencing tools for research interviews, including reducing geographical constraints associated with in-person interviews and offering greater opportunities to reach geographically dispersed participants. Several predetermined questions were prepared prior to the interview. These questions were administered to individuals involved in software development and the internal stakeholders or users of the DBNMS. The interview guide included questions that explored their inputs, experience, insights, and suggestions for improving the use of privacy engineering in software development through the development and implementation of the DBNMS.

Sampling involved selecting a representative subset of the target population for the study. A purposive sampling method was chosen due to its versatility and ability to save time and expense while gathering data. These techniques aimed to provide researchers with as much information as possible on the vital subject under study (Baiju, 2022).

In this case, the target population for internal stakeholders consisted of ten (10) individuals from the National Privacy Commission who had been involved in the development of the DBNMS. These individuals were the only ones involved in the DBNMS development within the Commission and possessed the most familiarity with the system's feature.

External stakeholders or users of the DBNMS were also invited as participants in the study. Each DBNMS user holds different views and knowledge, involving external individuals helped gather information from other perspectives. These views can reveal privacy issues, usability problems, and weaknesses that internal developers might have overlooked. In addition, external users make it easier for testing the DBNMS under real life conditions. It is essential for assessing the performance of the system under different circumstances and locating hidden defects or loopholes that could manifest themselves only once deployed. Finally, since the study focused on the privacy solutions achieved through privacy engineering techniques, compliance validation is important. External users who are experts in data protection regulations and privacy laws can help verify the system's compliance with relevant legal requirements especially with the requirements of the Data Privacy Act of 2012, its Implementing Rules and Regulation, and the issuances of the National Privacy Commission. This is critical for ensuring that the DBNMS meets the standards set by the National Privacy Commission and other regulatory bodies. For this reason, two (2) external users of the DBNMS were also invited to participate in this study. These external stakeholders or users should have been familiar with the functions and purpose of the system, having used it for at least six (6) months. The researcher decided to invite only two (2) external stakeholders due to the limited criteria and because the study focused more on the development process using privacy engineering techniques, in which external users had no involvement. External users were invited to provide comments on the outcome of the development process, which followed privacy engineering techniques.

The sample size was chosen considering the development phase of the DBNMS. During development, only a few NPC personnel were involved. Similarly, there were only a limited number of external participants the researcher could invite for the study. In total, twelve (12) participants were invited for interviews for data collection purposes. The researcher believes the chosen sample size was sufficient to achieve data saturation for this study. According to a LinkedIn article by Underwood (2023), some studies are successful with as few as 10 participants. However, this depends heavily on the quality of screening and recruiting the most appropriate participants, as well as the industry of the study.

➢ *The Criteria used in Selecting the Participants are as follows:*

- *Internal Stakeholders (NPC Personnel)*

✓ Should have participated in the development of the DBNMS.
✓ Should have knowledge in cyber security and privacy.
✓ Participants that are considered internal stakeholders or internal users and have background in software development who are part of the development of the DBNMS should be familiar with different software development frameworks such as but not limited to Agile, SDLC, etc.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

- ✓ Should be familiar with Privacy by Design, etc.

- *External Stakeholders (Organizations)*

- ✓ Should have used the DBNMS and familiar with its function particularly those who have been using the system for at least six months.
- ✓ Should be knowledgeable with information security and privacy concepts especially with the requirements of the Data Privacy Act of 2012, its Implementing Rules and Regulation and the issuances of the National Privacy Commission.
- ✓ Should be in the Privacy sector for more than a year.

To avoid participant bias, the researcher requested confirmation from the participants if the transcribed audio interview is correct and accurate. In addition, the researcher engaged in reflexivity to acknowledge personal biases and to ensure the diversity of participants, the purposive sampling based on key characteristics stated earlier. Also, the researcher analyzed the codes systematically and documented the findings transparently.

D. Instrument

An interview guide was developed and used during interviews with selected participants. These questions were a mix of open-ended and multiple-choice formats. The participants were individuals who had been involved in the development of the DBNMS, including both internal end-users and external users of the system. The interview guide explored participants' insights, suggestions, and experiences related to the effectiveness of the privacy engineering techniques implemented during the DBNMS software development stages. The questions were also designed to capture participant input on ways to improve the use of privacy engineering methods. This information could then be used to develop guidelines for software development or engineering within the National Privacy Commission for future software projects.

Several interview questions were crafted following the ISO 25010:2015 standard, Systems and software engineering — Systems and software Quality Requirements and Evaluation (Square) — System and software quality models, with a focus on the security aspect. An article by Rebes (2019) suggests that ISO 25010 provides a valuable framework for defining software metrics important for a specific project. It is not intended to be an exhaustive roadmap, but rather a guide that can be adapted based on specific circumstances. In this case, the security aspect of the standard informed the development of the interview questions, aligning with the study's aim to gather evidence about the effectiveness of privacy engineering techniques in enhancing software security and privacy. The interview guide was then validated by an external security expert to ensure the effectiveness of the data gathering process. The researcher obtained a certification from the expert as verification of this validation process.

E. Data Analysis

This section describes how the data collected from interviews were analyzed and used. The data analysis involved the following activities: Transcription of the interview recordings, Coding and thematic analysis using inductive and causal reasoning approaches. Thematic analysis, as described by Caulfield (2022), is a method for analyzing qualitative data. It's a valuable approach for research that aims to understand people's views, opinions, knowledge, experiences or values based on a set of qualitative data. For the coding process, an inductive reasoning approach was employed, which Bhandari (2022) defines as a logical method for drawing inferences or conclusions. This approach helped identify whether the privacy engineering techniques implemented during the DBNMS software development were effective in implementing appropriate privacy and security measures.

F. Limitations

The results of this study were not intended to provide conclusive evidence regarding the effectiveness of privacy engineering techniques in software development. Due to the limitations of the data collection method, which focused solely on internal DBNMS stakeholders, the data analysis using the chosen research design and methodologies may be considered lacking in generalizability. This research is intended to inform the National Privacy Commission's own software development strategies.

G. Establishing Trustworthiness

To validate the results of the findings, the researcher applied the four general criteria of approach to trustworthiness: credibility, transferability, dependability, and confirmability. As Billups (2021) explained, trustworthiness, a concept introduced by Lincoln and Guba (1985), is considered the quintessential framework for evaluating qualitative research. It consists of four elements: credibility (truth), dependability (consistency), transferability (applicability), and confirmability (neutrality. The following strategies were employed to address each criterion:

Credibility – a member checking approach was used to establish the credibility of the findings. Participants received copies of their interview transcripts to verify factual accuracy and confirm their original statements. According to Politz (2023), this collaborative technique (member checking) goes beyond validating data and addressing ethical concerns. It can also enhance the overall richness of data by incorporating participants' firsthand information or insights into the study.

Dependability – Detailed description of the research methods used in this research is added to this study to ensure and establish dependability and reliability of the procedures taken by the researcher. According to Shenton, in order to address the dependability issue more directly, the processes within the study should be reported in detail, thereby enabling a future researcher to repeat the work, if not necessarily to gain the same results. Thus, the research design may be viewed as a "prototype model" (Shenton, 2004).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

Transferability – this criterion can be established through the use of thick description, according to Billups, Thick description allows the researcher to more easily evaluate how this same circumstance of people, place, and phenomenon could be applied in a similar setting, under similar conditions, with similar participants (Billups, 2021). To apply transferability effectively, readers need to know as much as possible about the original research situation in order to determine whether it is similar to their own. Therefore, researchers must supply a highly detailed description of their research situation and methods (Barnes et al., 2005).

Confirmability – To achieve this, the researcher used the following techniques mentioned in the Queens University of Charlotte online: Taking notes regarding personal feelings, biases and insights immediately after an interview and following, rather than leading, the direction of interviews by asking for clarifications when needed (University of Charlotte, 2022).

H. Ethical Consideration

This study adhered to ethical principles such as informed consent and confidentiality. Data collection and handling procedures ensured the language used was appropriate to the participants' known dialect, such as English. Furthermore, the data collection process complied with Republic Act 10173 or the Data Privacy Act of 2012, its implementing rules and regulations, as well as the issuances of the National Privacy Commission. Participation in the study was voluntary and by no means has the researcher coerced participants into providing their personal data and participation in the study. Prior to the interview, an Informed Consent Form (ICF) from the Holy Angel University was sent to the participants' email addresses. Participants who agreed to participate signed and returned the ICF to the researcher. Participation remained entirely voluntary, and participants could withdraw from the study or delete any information they provided at any point without consequences. They also have the right to refuse future storage of their data for use in future studies.

Also, the study findings may be presented in a research forum or published in a journal. Before the findings are made widely available to the public, each participant has the option to receive a summary of the results. The summary will be presented in an aggregate form, and participants are anonymized to protect their identity and privacy. This format will allow participants to open using a spreadsheet application such as Microsoft Excel. Participants can exercise all these options by contacting the researcher through the email address or contact information provided in the ICF and email invitation.

Participation in this study may have involved minimal or low risks. For example, participants might have felt some discomfort answering personal or sensitive interview questions, although this discomfort would not be directly attributable to the study itself. Throughout the study, participants had the right to withdraw without consequences. In addition, the potential vulnerability of participants, such as their inability to provide informed consent, was considered low risk. This vulnerability was mitigated by sending the ICF to participants before data collection or interviews. The email containing the ICF explained the study's title, objectives, desired outcomes, and possible risks. These details were also reviewed with participants before the interview began. These measures aimed to prevent any vulnerability or risk, however unlikely.

Moreover, the researcher explained the potential benefits of the study's impact to participants. This includes how their participation will contribute to advancing the understanding of how privacy engineering can improve the security and privacy of software systems. It is also important to acknowledge that a possible conflict of interest for participants could exist, however unlikely. This conflict might arise if some participants are involved in competing projects or products that could benefit from downplaying the effectiveness of the Data Breach Notification Management System (DBNMS). This could be motivated by a desire to promote their own project's success or hinder the success of a competing solution. However, the possibility of this scenario is considered to be very low.

While the researcher was employed in the National Privacy Commission, there is no conflict of interest even though data collection was involved. First, the study was conducted independently by the researcher following the requirements of the course. While the system in question is from the National Privacy Commission, collecting data for the capstone project aligns with the NPC's mission of promoting and protecting privacy rights. There is no inherent conflict as the project served the same goals. In addition, the data collection process adhered to strict ethical guidelines, such as informed consent, data anonymization, and confidentiality assurances. These safeguards can minimize any perceived or real conflicts of interest. Moreover, the researcher did not gain personally or professionally from the outcomes of the research, and the data collection was solely for academic purposes and did not impact his career or compensation, thus indicating a lack of conflict of interest. Finally, this study was not sponsored by the NPC, or any other institution. All expenses pertaining to the study were shouldered solely by the researcher.

By adhering to these ethical considerations, the research study aimed to protect the rights and well-being of participants, maintain their confidentiality and anonymity, obtain informed consent, and ensure the security of collected data. These measures contributed to upholding the principles of ethical research conduct, fostering trust, and privacy considerations. In addition, this paper underwent review of the Holy Angel University Institutional Review Board and received approval prior to the collection of data from the participants.

V. RESULTS

In this section, the results of the study are presented. The data collected from the participants through a semi-structured interview were analyzed following the thematic analysis approach. Interview recordings were transcribed and then

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

analyzed with the help of a web-based qualitative analysis tool named Quirkos. Quirkos is a web-based qualitative software analysis tool that the researcher subscribed to in order to make analysis more efficient. Prior to the use of the software, interviews were conducted through an online meeting application. Meeting interviews were then transcribed and anonymized prior to uploading to the said software. Using the thematic analysis approach, coding and generation of themes were done using the software. The themes were developed firstly by choosing or grouping similar statements from the participants into codes. The researcher then repeated this process until all statements were carefully grouped into their proper codes. After completing the codes, the researcher then further classified the codes into what became the themes.

Table 1 presents a summary of the themes and their description. Careful analysis of interview transcripts has generated eight (8) themes and twenty-five (25) codes. The table shows the themes and their meanings. The researcher reviewed each interview transcript to ensure the quality of findings that resulted from the analysis.

Table 1 Table of Themes

Themes	Meaning
Stakeholder Background	This theme explores the diverse backgrounds, roles, and interests of participants involved in the study. Their different roles be it external or internal users of the DBNMS, shedding light on their varied perspectives and motivations
Privacy Engineering Benefits	This theme delves into the advantages and positive outcomes associated with integrating privacy engineering practices into the software development process particularly in the DBNMS.
Importance of stakeholder involvement	This theme emphasizes the significance of engaging stakeholders throughout the privacy engineering process, underscoring their contributions to decision-making, requirements definition, and accountability.
Comparison of Privacy Engineering and Privacy by Design	This theme examines the distinctions and similarities between privacy engineering approaches and the Privacy by Design framework, elucidating their respective principles, methodologies, and effectiveness in safeguarding privacy.
Importance of Privacy Measures	This theme underscores the critical role of implementing robust privacy measures in mitigating risks, safeguarding sensitive data, and upholding user privacy rights within systems and its importance early in the development stages of a system.
Level of Perception of DBNMS Protection	This theme explores stakeholders' perceptions and evaluations of Data Breach Notification Management System (DBNMS) assessing their effectiveness and adequacy in addressing privacy concerns
Privacy Challenges in Software Development	This theme discusses the obstacles, complexities, and ethical dilemmas encountered during software development processes, particularly concerning the integration of privacy features and compliance with regulatory requirements.
Lessons Learned	This theme reflects on the insights, experiences, and best practices gleaned from privacy engineering initiatives, offering valuable lessons and recommendations for improving future privacy-related endeavors and mitigating potential pitfalls.

Careful analysis of interview transcripts has generated eight (8) themes and twenty-five (25) codes. The leftmost column of the table signifies the number of codes within each theme. Some themes also contain sub-themes. The researcher reviewed each interview transcript to ensure the quality of findings resulting from the analysis. Below is the explanation for each theme:

A. *Objective 1: Evaluation of the Effectiveness of the Application of Privacy Engineering Techniques in Software Development.*

➢ *Themes that Addressed the Objective:*

- *Privacy Engineering Benefits*

This theme highlights the advantages of privacy engineering, which is divided into five codes: its importance, the problems it solves, its role in effective management, its universal application, and its process in software development. The application of privacy engineering in software development is highly effective and yields positive results. One participant noted a privacy issue related to report generation, and it was agreed that limiting report generation is the best way to integrate a feature without compromising privacy and security. Privacy and security risks in the development of the DBNMS were addressed through privacy engineering methodologies. An external stakeholder also recognized the importance of privacy engineering in software engineering, stating that it embeds privacy principles into software systems, identifies and addresses privacy risks, implements robust security measures, and ensures compliance with data protection regulations.

- *Importance of Privacy Measures*

This theme is a collection of statements from participants that capture their views on the importance of privacy measures in software development. The participants emphasized the need for new ways on how to solve privacy and security measures brought about by the ever changing technological and regulatory landscape. One participant stated that the need to formulate and implement new privacy

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

preserving methodologies is relevant because of the ever-changing landscape in the cyber world.

Another participant highlighted the effectiveness of integrating privacy engineering techniques during the development of the DBNMS, he stated that during the system development of the DBNMS, weak authentication mechanisms exposed user accounts to potential breaches or unauthorized access, and it was identified during the Privacy Impact Assessment and because of this, the team worked on strengthening authentication protocols by implementing multi-factor authentication (MFA) and regularly updating authorization practices.

- *Lessons Learned*

This theme is composed of lessons learned during the development of the DBNMS particularly with the application of privacy engineering techniques during the said activity. The importance of integrating privacy engineering techniques during software development was considered as stated by one of the participants according to him, he has witnessed the importance of having guidance in privacy engineering when developing systems and that the current project of publishing a privacy engineering advisory would greatly help and encourage organizations and developers to integrate privacy into their systems.

- *Perception of level of Privacy Protection*

Participants perceive the DBNMS as having strong privacy protection, with successful integration of privacy considerations via privacy engineering methodologies. Integration of privacy considerations is successful when a system passes necessary security privacy tests and validations. Positive feedback includes visible privacy principles, upheld individual privacy rights, evidence of risk assessment such as PIA, and adequate cyber security. Navigation of the DBNMS reveals its privacy-conscious development. Since the DBNMS's launch, no security incidents or complaints about data protection and privacy rights have been reported, indicating successful privacy and security integration. The absence of negative feedback about the system's privacy and security from external stakeholders further supports this.

- *Comparison of Privacy Engineering and Privacy by Design*

Privacy engineering's effectiveness in software development was highlighted by comparing it to the Privacy by Design approach. While Privacy by Design is popular and required by the GDPR, operationalizing its requirements is challenging. One participant noted that privacy remains a concept in software under Privacy by Design, but privacy engineering bridges this gap by implementing these concepts into practice. The application of privacy engineering techniques in the DBNMS development is viewed positively based on participant feedback. Both internal and external participants agree on the importance of applying privacy engineering techniques during software development.

B. Objective 2: To identify the factors that contribute to the success or failure of privacy engineering techniques in software development at the NPC.

➢ *Themes that Addressed the Objective:*

➢ *Lessons Learned*

During the DBNMS development, lessons were learned that contribute to the success or failure of privacy engineering techniques in software development. A key lesson stated by a participant is the importance of involving all stakeholders, especially the legal team, in the development process. This involvement ensures that appropriate privacy measures are integrated into software systems. It is particularly crucial when translating legal requirements into functional code. The participation of the Commission's legal team in software development is deemed necessary. This sentiment is echoed by another participant, emphasizing the essential role of the legal team in ensuring that suitable privacy measures are incorporated into software systems.

➢ *Privacy Challenges in Software Development*

The rapid development of technology poses significant challenges for privacy in software development, with threats constantly evolving according to a participant. He added that stakeholders must adopt appropriate measures to address these challenges. Additionally, changing privacy requirements add complexity, requiring constant vigilance to keep protection settings up to date. Interpreting privacy laws for implementation in software further complicates matters, leading to potential confusion and delays another participant emphasized. Another participant mentioned about the scarcity of privacy engineering and cybersecurity experts, hindering the implementation of necessary measures. Lack of sufficient funds exacerbates these challenges, potentially preventing solutions from being realized. In summary, factors affecting privacy engineering in software development include stakeholder engagement, technological advancements, regulatory interpretation difficulties, expert scarcity, and budget constraints.

In summary, for objective number 2, the factors that contribute to the success or failure of privacy engineering techniques in software development within the Commission that were identified are the following:

- Factor 1: Stakeholder engagement
- Factor 2: Rapid advancement of Technology
- Factor 3: Difficulty in the interpretation of regulations, particularly privacy laws
- Factor 4: Scarcity of Privacy Engineering experts
- Factor 5: Scarcity in the cyber security field experts
- Factor 6: Lack of funds

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

C. Objective 3: To provide guidance on how to effectively integrate privacy and security in software engineering within the National Privacy Commission based on the conclusion that will be presented in this study. A software development guide with the methodologies on how to integrate privacy engineering to the software development life cycle will be developed to be used by NPC engineers.

➢ *Themes that Addressed the Objective:*

- *Lessons Learned*

One participant stressed the importance of having guidelines for the development of systems in the Commission. According to him he witnessed the importance of having guidance in privacy engineering when developing systems and that the Commission's current project of publishing a privacy engineering advisory would greatly help and encourage organizations and developers to integrate privacy into their systems. Although this is not the guideline that is intended for the objective, the importance of having clear guidance is emphasized.

In the same theme, another participant mentioned that the experiment with the DBNMS served as a learning opportunity for NPC engineers and that the project can serve as a guideline for future projects, he stressed that the DBNMS can serve as the baseline for any other future projects for system development that would like or should carry on privacy engineering methodologies or techniques in developing a system since this is one of the major projects of the Commission that really pushed through implementing privacy engineering technologies starting from the internal stakeholder engagement and privacy impact assessment.

In summary, a software development guide is drafted to guide NPC engineers of future software development projects. This guideline will be used only for internal use and will not be published for public consumption and will also be subject to review and approval of the Commission.

VI. DISCUSSIONS

The following section details the discussion of the findings in this study. After carefully considering and reviewing the generated themes and codes, the result of the analysis is discussed in this section including the conclusion and recommendations for future research.

The result of this study is essential in achieving the objectives. By analyzing and reviewing the data collected from the semi-structured interviews, the researcher evaluated the effectiveness of implementing privacy engineering techniques in software development. In a similar note, one study emphasized the importance of privacy engineering in software development. It stated that Privacy Engineering integrates privacy considerations into software and systems engineering methods, ensuring that privacy is a fundamental aspect of the design and development process. This approach helps in creating products that prioritize data protection and privacy (Martin & Kung, 2018). In addition, the result of the analysis and review of data provided insights about the factors that contribute to the success and failure of implementing privacy engineering in software development. These factors were identified and enumerated in this study. According to Nurgalieva et al., The adoption and implementation of privacy and security practices in software development are influenced by organizational and individual behavior, highlighting the importance of addressing these aspects for successful integration (Nurgalieva et al., 2023). In a study made by Campanille, et al., there is a need for methodological effort to systematically adapt software development to privacy regulations (Campanile et al., 2022). Because of this result, the need for a more detailed guide on how to develop a privacy compliant and secure software system is strengthened. Similar to one of the objectives of this study, the need for a development of a more privacy centered software development guide was echoed in different research papers. Researchers from the University of Brasilia proposed a reference guide to assist ICT professionals in understanding and implementing the principles of the Data Privacy Law of Brazil (LGPD) (Rocha et al., 2023). In another study, it provides a different approach which is to fund independent academic research groups or not-for-profits to build tangible and understandable guides for the developer community (Tahaei et al., 2023).

➢ *Reflexivity*

This study revolves around the role of privacy engineering in software development and uses a DBNMS to measure its effectiveness in ensuring that privacy requirements and security are integrated into a software system during development. Due to the researcher's dual role as a privacy professional and information technology professional, achieving complete objectivity and setting aside personal biases can be challenging. The researcher's work as an Information Technology Officer in the National Privacy Commission involves the evaluation and initial review of personal data breaches reported by organizations, wherein during these activities, he gained experience on how personal data breaches take place including those that resulted from the lack of security and privacy measures in systems as well as incorrect implementation of these measures. In addition, part of his work involves the conduct of compliance check audits wherein the researcher is involved in visiting organizations and auditing or checking their compliance requirements in relevance to the DPA of 2012, its IRR and issuances of the Commission. There are instances wherein privacy requirements were not properly implemented nor correctly interpreted. This leads the researcher to believe that engineering privacy into systems and processes is not only the sole responsibility of the Information Technology team but also with all stakeholders involved in the processing system including the legal team. Moreover, the researcher is also a privacy professional and is a Certified Information Privacy Technologist certified by the International Association of Privacy Professionals. The researcher's dual roles may have introduced bias or conflicts of interest. For example, the researcher may be inclined to have bias over the benefits and positive impact of implementing privacy engineering in software development over other methodologies. Thus, the researcher's opinion and his personal background may have influenced the interpretation of data. However, to ensure that

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

interpretation of data is as objective as possible, confirmation of transcribed data from the participants was conducted. The participants' opinion and answers to the research questions were accurately transcribed following their confirmation.

VII. CONCLUSION

In conclusion, the results of this study confirm that integrating privacy engineering into software development processes is essential for ensuring user data protection and compliance with privacy regulations. This study employed semi-structured interviews with participants selected using purposive sampling. The collected data was then analyzed and evaluated using thematic analysis. Key findings of the study show the importance of integrating privacy engineering techniques in software development. Following the data collection process, a majority of the participants agreed that such integration is crucial for a privacy-compliant and secure software system. These sentiments are echoed in studies conducted by various researchers, as identified in the related literature review. To ensure successful integration, this study also identified factors that contribute to its success. These factors include: stakeholder engagement, rapid technological advancement, difficulty in interpreting regulations (particularly privacy laws), scarcity of privacy engineering and cybersecurity experts, and lack of funds. Similar factors were identified by researchers in related studies on privacy integration in software development. Finally, to guide NPC engineers for future projects, a software development guide was developed as one of the study's objectives. This guide leverages the study's results to identify key privacy requirements and methodologies for implementing privacy engineering in the Commission's future software projects.

RECOMMENDATION AND DIRECTION FOR FUTURE RESEARCH

The findings in this study may not be sufficient to cover all the aspects of the implementation of privacy engineering in software engineering. One important point to consider is that there are different approaches to software development, some might follow the old Software Development Life Cycle (SDLC) method or developers might follow a newer approach such as the agile methodology. It is important to note that even the agile methodology can be done in different approaches. This alone may provide future researchers with subjects to topics pertaining to privacy engineering in software development. In addition, the sample size may be too small for other researchers, future researchers may want to consider gathering data from a much larger size of participants. Moreover, different requirements on specific data protection regulations such as but not limited to the General Data Protection Regulation (GDPR), the Personal Data Protection Act of 2012 of Singapore, etc. can be used as a subject basis for privacy engineering if software systems to be developed may need to comply with the stated privacy laws.

Lessons learned from this study can also be valuable for future research. One notable example is the importance of collaboration among different stakeholders during software development. Without input from privacy experts, the legal team, and other stakeholders, privacy requirements may not be successfully integrated into software projects. Also, the identified factors that may contribute to the successful implementation of privacy engineering techniques in software development should be considered. Management support is essential to foster a culture of privacy and successful integration of privacy requirements in software projects. Continuous learning and development are necessary to ensure that updated privacy and security requirements are followed and implemented in software projects.

Finally, another direction for future studies could involve exploring latest techniques in secure software development. Future researchers may conduct studies using different Privacy Enhancing Technologies (PETs), such as differential privacy and homomorphic encryption, to investigate how these PETs can be applied to privacy engineering in software development. Technology and threats evolve rapidly, so developers and security professionals need to adapt and continuously improve. The latest trends in secure coding should be considered whenever privacy engineering in software development is discussed.

ACKNOWLEDGEMENT

First and foremost, I would like to express my gratitude and appreciation to our Lord God for providing me the strength, knowledge, and all necessary resources to successfully complete this project.

I would like to express my deepest appreciation to our Dean, Dr. Marlon Tayag and Dr. Alma Theresa D. Manaloto for providing me with the opportunity to complete this paper and for inspiring me to finish this research paper.

I am deeply thankful to the oral examiners, to the Defense Panel Chair, Professor Kevin Aldrin Espinosa, Attorney Paul Edgar Villarosa and Dr. Joseph Esquivel whose guidance, recommendations and insights has given the paper a level of depth and clarity that I could not have achieved on my own. Their feedback and suggestions were crucial in refining my research and analysis.

I'm extremely grateful to the National Privacy Commission, for allowing me to complete my studies while doing my functions in the Commission. I am deeply indebted to Attorney Rainier Anthony Milanes, for allowing me to use the DBNMS for my research paper.

This endeavor would not have been possible without the help of my adviser, Professor Avigail P. Magbag whose unwavering support, invaluable guidance, and expert insights have been instrumental throughout this research journey. Her expertise has been invaluable in shaping my understanding and refining my arguments.

I would also like to extend my sincere appreciation to Dr. Everly Chua, whose unwavering support and guidance ensured the smooth progression and successful completion of this research paper.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

To my colleagues and friends, to Kelvin, Walden, Janssen, Shaira, Grelly, Atty. Amor, Raymond, Jenille, Jobelle, Juvy, Darwin, and to those others who participated as research participants, including Joshue and Dr. Labung, words cannot express my sincerest gratitude for helping me in gathering the necessary information which allowed me to conduct a meaningful analysis to complete this paper.

I would also like to extend my appreciation to Professor Kimberly Pineda, to the Institutional Review Board and University Research Office and the rest of HAU's faculty for their honest review, guidance and recommendations to improve this paper.

Furthermore, I am extremely grateful to my friends and family for their unwavering support and understanding during this challenging yet rewarding journey.

Lastly, I could not have undertaken this journey without the support of my kind and loving wife Dr. Victoria Magdaong and my daughter, Radiant M. Dela Cruz, their belief in me has been a constant source of motivation.

I acknowledge the contributions of all the participants who generously shared their time and perspectives for this study. This project would not have been possible without the support and contributions of everyone mentioned above. Thank you all for your assistance and encouragement.

REFERENCES

[1]. Andrade, V. C., Gomes, R. D., Reinehr, S., Freitas, C. O., & Malucelli, A. (2022). Privacy by design and software engineering. Proceedings of the XXI Brazilian Symposium on Software Quality. https://doi.org/10.1145/3571473.3571480

[2]. Ayton, D., Tsindos, T., & Berkovic, D. (2023). Qualitative research: A practical guide for health and social care researchers and practitioners. Council of Australian University Librarians, Open Educational Resources Collective.

[3]. Barnes, J., Conrad, K., Demont-Heinrich, C., Graziano, M., Kowalski, D., Neufeld, J., Zamora, J., & Palmquist, M. (n.d.) (2005). Home. Generalizability and Transferability. https://writing.colostate.edu/guides/guide.cfm?guideid=65

[4]. Bhandari, P. (2022, December 05). Inductive Reasoning | Types, Examples, Explanation. Scribbr. Retrieved June 19, 2023, from https://www.scribbr.com/methodology/inductive-reasoning/.

[5]. Billups, F. D. (2021). Qualitative data collection tools: Design, development, and applications. SAGE Publications.

[6]. Britton, J. (2021, March 6). What is ISO 25010?. Perforce Software. https://www.perforce.com/blog/qac/what-is-iso-25010

[7]. Campanile, L., Iacono, M., & Mastroianni, M. (2022). Towards privacy-aware software design in small and Medium Enterprises. 2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). https://doi.org/10.1109/dasc/picom/cbdcom/cy55231.2022.9927958

[8]. Caulfield, J. (2022, November 25). How to Do Thematic Analysis | Step-by-Step Guide & Examples. Scribbr. Retrieved June 24, 2023, from https://www.scribbr.com/methodology/thematic-analysis/

[9]. Cavoukian, A., Shapiro, S., & Cronk, R. J., Privacy engineering: Proactively embedding privacy, by design (2014). Toronto; Information and Privacy Commissioner, Ontario.

[10]. Cherry, C. (2022, May 20). What Is Naturalistic Observation? November 20, 2023, https://www.verywellmind.com/what-is-naturalistic-observation-2795391

[11]. Dulberg, R. (2021, September 10). An Engineer's Guide to Privacy by Design. medium. August 20, 2023, https://medium.com/codex/an-engineers-guide-to-privacy-by-design-f487d16dcbbc

[12]. Falconer, S. (2022, January 27). Software Engineering's Next Great Challenge: Data Privacy. www.Skyflow.com. https://www.skyflow.com/post/software-engineerings-next-great-challenge-data-privacy

[13]. George, T. (2022). Semi-Structured Interview | Definition, Guide & Examples. Scribbr. https://www.scribbr.com/methodology/semi-structured-interview/

[14]. Ghosh, A. (n.d.). An insider look at real-world examples of cloud hacks. LinkedIn. https://www.linkedin.com/pulse/insider-look-real-world-examples-cloud-hacks-aritra-ghosh

[15]. Irani E. The Use of Videoconferencing for Qualitative Interviewing: Opportunities, Challenges, and Considerations. Clinical Nursing Research. 2019

[16]. King, N., Horrocks, C., & Brooks, J. (2019). 2nd Edition Interviews in Qualitative Research (2nd ed.). Sage.

[17]. Leonhardt, M. (2019, July 23). Equifax to pay $700 million for massive data breach. here's what you need to know about getting a cut. CNBC. https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html

[18]. Libguides: Qualitative Study Design: Sampling. Sampling - Qualitative study design - LibGuides at Deakin University. (2023, October 12). https://deakin.libguides.com/qualitative-study-designs/sampling#:~:text=While%20there%20are%20no%20hard,Creswell%20%26%20Creswell%2C%202018).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG877

[19]. Martin, Y.-S., & Kung, A. (2018). Methods and tools for GDPR compliance through privacy and Data Protection Engineering. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). https://doi.org/10.1109/eurospw.2018.00021

[20]. Meem, M. I. (2020, June 19). Importance of Epistemology and Ontology in Research Design and Methodology Mahabuba Islam Meem Mahabuba Islam Meem Research Assistant. November 19, 2023, https://www.linkedin.com/pulse/importance-epistemology-ontology-research-design-mahabuba-islam-meem/

[21]. Naidu, N. (2023, April 19). Software Engineering | Agile Software Development. geeksforgeeks. August 20, 2023, https://www.geeksforgeeks.org/software-engineering-agile-software-development/

[22]. National Institute of Standards and Technology, Brooks, S., Garcia, M., Lefkovitz, N., Lightman, S., & Nadeau, E., An Introduction to Privacy Engineering and Risk Management in Federal Systems (2017). National Institute of Standards and Technology. Retrieved August 22, 2023, from https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[23]. Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. International Journal of Qualitative Methods, 16(1). https://doi.org/10.1177/1609406917733847

[24]. Nurgalieva, L., Frik, A., & Doherty, G. (2021). Review of WiP: factors affecting the implementation of privacy and security practices in software development: a narrative review. https://www.leysannurgalieva.com/publications. Retrieved 2023, from https://www.leysannurgalieva.com/publications.

[25]. Nurgalieva, L., Frik, A., & Doherty, G. (2023). A narrative review of factors affecting the implementation of privacy and security practices in software development. ACM Computing Surveys, 55(14s). https://doi.org/10.1145/3589951

[26]. Office, U. S. G. A. (n.d.). Data Protection: Actions taken by Equifax and federal agencies in response to the 2017 breach. Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach | U.S. GAO. https://www.gao.gov/products/gao-18-559

[27]. Park, C. (2020, March 20). How “Notice and Consent” Fails to Protect Our Privacy. New America. August 20, 2023, https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/

[28]. Politz, D. (2023, August 29). Member check and respondent validation in qualitative research. Delve. https://delvetool.com/blog/member-check-respondent-validation

[29]. Queens University of Charlotte (2022, May 12). A guide to qualitative rigor in research: Queens University Online. Queens University of Charlotte. https://online.queens.edu/resources/article/guide-to-qualitative-rigor-in-research/

[30]. Rebes, P. (2019, August 13). Software Quality Standards—How and Why We Applied ISO 25010. Retrieved August 12, 2023, from https://www.monterail.com/blog/software-qa-standards-iso-25010.

[31]. Rocha, L. D., Caneda, E. D., & Sousa Silva, G. R. (2023). Privacy Compliance in Software Development: A Guide to Implementing the LGPD Principles (thesis). Association for Computing Machinery, New York.

[32]. Sampath, S. (2022, February 11). What is Privacy Engineering and how does it act as an enabler of Digital Innovation? https://www.linkedin.com/pulse/what-privacy-engineering-how-does-act-enabler-digital-sampath/

[33]. Sangaroonsilp, P., Dam, H. K., & Ghose, A. (2022b). Common privacy weaknesses and vulnerabilities in software applications. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4025928

[34]. Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. Education for Information, 22(2), 63–75. https://doi.org/10.3233/efi-2004-22201

[35]. Spiekermann-Hoff, S. (2012). The Challenges of Privacy by Design. Communications of the ACM (CACM), 55(7), 34 - 37. https://doi.org/10.1145/2209249.2209263

[36]. Stahl, N. A., & King, J. R. (2020). Expanding Approaches for Research: Understanding and Using Trustworthiness in Qualitative Research. Journal of Developmental Education, 44(1), 26–28. http://www.jstor.org/stable/45381095

[37]. Stanke, B. (2022, December 18). Feature-Driven Development: The Pros, Cons, and How It Compares to Scrum. bobstanke. August 20, 2023, https://www.bobstanke.com/blog/feature-driven-development

[38]. Tahaei, M., Vaniea, K., & Rashid, A. (2023). Embedding privacy into design through software developers: Challenges and solutions. IEEE Security & Privacy, 21(1). https://doi.org/10.1109/msec.2022.3204364

[39]. Thomas, F. B. (2022). The Role of Purposive Sampling Technique as a Tool for Informal Choices in a Social Sciences in Research Methods.

[40]. Underwood, T. (2023, April 26). How to Choose a Sample Size in Qualitative Research. Retrieved August 12, 2023, from https://www.linkedin.com/pulse/how-choose-sample-size-qualitative-research-focusinsite.

[41]. Velimirovic, A. (2022, November 17). What is SDLC? Software Development Life Cycle Defined. PhoenixNap. August 20, 2023, https://phoenixnap.com/blog/software-development-life-cycle