INVESTIGATING THE ADAPTATION OF PRIVACY BY DESIGN IN SOFTWARE AIMED AT SRI LANKAN END USERS

Witiyala Kuruppu Arachchilage Geethani Subhashani

219159D

Degree of Master of Business Administration in Information Technology

Department of Computer Science and Engineering
Faculty of Engineering

University of Moratuwa
Sri Lanka

June 2025

INVESTIGATING THE ADAPTATION OF PRIVACY BY DESIGN IN SOFTWARE AIMED AT SRI LANKAN END USERS

Witiyala Kuruppu Arachchilage Geethani Subhashani

219159D

The dissertation was submitted to the Department of Computer Science and Engineering of the University of Moratuwa in partial fulfilment of the requirement for the Degree of Master of Business Administration in Information Technology.

Department of Computer Science and Engineering
Faculty of Engineering

University of Moratuwa
Sri Lanka

June 2025

DECLARATION

I declare that this is my own work and this thesis does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

W K A Geethani Subhashani Date:20/06/2025

Signature of the candidate

The above candidate has carried out research for the Masters thesis under my supervision.

Dr. Sandareka Wickramanayake Date: 20/06/2025

Signature of the Supervisor

Dr. Thusitha Abeysekara Date: 20/06/2025

Signature of the Co-Supervisor

COPYRIGHT STATEMENT

ACKNOWLEDGEMENT

This thesis marks the completion of my Degree of Master of Business Administration in Information Technology at University of Moratuwa. I would like to take this opportunity to express my deepest gratitude to all who have contributed to the successful completion of this study.

First and foremost, I wish to express my profound gratitude to Dr.Sandareka Wickramanayake, my academic supervisor, for their invaluable guidance and constructive feedback throughout this research process. I want to thank my co-supervisor Dr. Thusitha Abeysekara for your insightful guidance on IT law, which greatly enriched my research study.

I wish to thank all the interview respondents who engaged in my study to share their experiences and expertise. Their contribution played a key role in shaping the findings of this research study.

Finally, I would like to express my heartfelt thanks to my family for the unwavering support and encouragement.

ABSTRACT

Software across desktop, mobile, web, and Internet of Things (IoT) technologies have evolved into powerful tools for customization and understanding user preferences which in turn collect vast amounts of user data. Consequently, organizations and governments worldwide have emphasized the importance of safeguarding user privacy through legal frameworks and principles such as Privacy by Design (PbD). PbD is a proactive approach that integrates privacy considerations into systems and processes from the outset rather than as an afterthought. While several studies have explored the integration of PbD in software development across different countries, there is a lack of research examining how Sri Lanka's software industry adapts these principles. With the recent enactment of Sri Lanka's Personal Data Protection Act (PDPA), software development firms are increasingly required to incorporate privacy and data protection measures. However, achieving a comprehensive approach necessitates going beyond regulatory compliance. This study investigates how software companies in Sri Lanka integrate PbD principles into the Software Development Life Cycle (SDLC) to ensure customer data privacy. A qualitative research design was adopted to gain in-depth insights into privacy considerations in software development. Data were collected through semi-structured interviews with seven experienced professionals working in medium-to-large-scale software firms or leading their own companies. Thematic analysis was employed to identify key themes related to privacy, privacy regulation, privacy design, and privacy embedding within the SDLC. Findings indicate that Sri Lankan software developers possess a strong understanding of privacy and legal compliance, particularly in relation to the PDPA. However, opinions remain divided regarding the implementation of pseudonymization and data encryption due to the associated costs and complexities, despite legal recommendations. Privacy embedding was found to be influenced by PbD principles, though not all principles are universally applied across contexts. The most commonly implemented privacy protection measures include data minimization and access control mechanisms. Additionally, the study highlights a trade-off between privacy and software performance, where excessive privacy measures can impact system efficiency and usability. This research contributes to the global discourse on privacy-aware software development by providing the first empirical insights into how the Sri Lankan software industry adapts PbD principles. The findings offer practical implications for industry professionals and policymakers seeking to enhance privacy integration within software development practices in emerging markets.

Keywords: Privacy, Privacy by Design, Data Encryption

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Description
API	Application Programming Interface
CCPA	California Consumer Privacy Act
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessments
DPO	Data Protection Officer
EU	European Union
EULA	End User License Agreement
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HSTS	HTTP Strict Transport Security
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
PbD	Privacy by Design
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDPL	Sri Lankan Data Protection Law
TLS	Transport Layer Security

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background

Software applications, spanning online, mobile, desktop, and Internet of Things (IoT) platforms, have emerged as powerful tools for personalizing services and understanding user needs by collecting large volumes of personal data. Personal data refers to any information that can be used to identify an individual, either directly or indirectly. Common examples include names, addresses, and identification numbers. Less obvious identifiers may include IP addresses, system configurations, and electronic document metadata. Moreover, personal data extends to information that, when combined with other identifiers, can reveal an individual's identity.

The increasing drive to monetize personal information and derive new insights from data collection has raised ethical concerns about its unregulated use and potential misuse. Therefore, there is a pressing need to establish robust privacy frameworks that strike a balance between safeguarding user privacy and supporting corporate interests. One promising approach is the adoption of Privacy by Design (PbD), a concept aimed at embedding privacy considerations into the early stages of the software development lifecycle (Cavoukian, n.d). By integrating privacy mechanisms from the outset, organizations can enhance the security and transparency of their products, processes, and applications.

The seven principles of PbD provide a structured framework for embedding privacy into technologies, practices, and procedures. These principles emphasize proactive measures to prevent privacy violations by ensuring that strict privacy standards are upheld across IT systems and business processes. Key aspects include presumption of privacy, data minimization, purpose specification, collection limitation, and use, retention, and disclosure Limitation. PbD promotes the automatic protection of personal data throughout its entire lifecycle, from collection to disposal, using techniques such as encryption, access control, secure data destruction, and activity logging. Moreover, visibility, transparency, accountability, and compliance are integral to ensuring alignment with stated privacy objectives.

In the context of Sri Lanka, personal data protection is increasingly recognized as a critical concern. The Personal Data Protection Act, No. 9 of 2022 serves as the primary legislation governing personal data processing in Sri Lanka. This Act applies to both local and foreign entities that process the personal data of Sri Lankan citizens (Parliament of Sri Lanka, 2022). However, unlike the General Data Protection Regulation (GDPR) enforced in the European Union (EU), Sri Lanka's Personal Data Protection Act does not explicitly mandate privacy by design principles. Notably, the GDPR's Recital 46 underscores the importance of incorporating technological and

organizational safeguards into the design of data processing systems to ensure privacy compliance (Intersoft Consulting Services AG, 2018).

Despite existing regulations, concerns have been raised regarding the implementation and effectiveness of these laws. In particular, the Sri Lankan software development sector lacks clear guidance on adopting privacy-enhancing technologies and integrating PbD principles into software development processes. This research aims to explore these gaps, investigate current practices, and identify barriers to the adoption of PbD within the Sri Lankan software industry.

1.1.1 Motivation

Implementing PbD in software development processes offers significant benefits for IT companies, despite the common misconception that it is a complex and burdensome compliance requirement. Many organizations perceive privacy regulations as a regulatory hurdle, often overlooking the potential strategic advantages PbD can provide. However, integrating privacy considerations into the early stages of development not only ensures regulatory compliance but also enhances efficiency, transparency, and user trust.

By embedding privacy into the design phase of software development, companies can proactively identify and mitigate risks, preventing costly revisions and ensuring robust data protection measures from the outset. This proactive approach fosters greater accountability and builds long-term trust with data subjects, which is crucial for businesses handling sensitive personal data. Although Sri Lanka's Personal Data Protection Act, No. 9 of 2022 does not explicitly mandate technical implementations of PbD, adopting these principles can position Sri Lankan IT companies as privacy-conscious leaders, enhancing their competitiveness in global markets.

In light of these considerations, there is a pressing need to investigate the current adoption of PbD within Sri Lanka's software development sector, identify barriers to its implementation, and explore best practices to empower organizations in building privacy-respecting technologies.

1.1.2 Research Scope

This study aims to investigate the adoption of Privacy by Design (PbD) within the Sri Lankan software development sector, focusing on how privacy can be integrated into the early stages of the software development lifecycle and examining the business implications of doing so. While PbD frameworks have been extensively explored in global contexts, limited research has been conducted on their application in Sri Lanka, particularly in software applications that process personal data of Sri Lankan data subjects.

The scope of this study is confined to the Sri Lankan software development industry, with a focus on applications handling personal data. Data collection is comprised of

primary and secondary data sources. As the primary data collection method, the researcher conducts semi-structured interviews with seven participants possessing extensive knowledge and practical experience in the field, ensuring diverse insights into PbD adoption. As the secondary data collection method, the researcher gets the help of library-based resources to enrich the analysis and contextualize findings.

This study seeks to address the knowledge gap surrounding PbD implementation in Sri Lanka's software industry while contributing valuable insights into best practices and challenges faced in adopting privacy-centric development approaches.

1.2 Problem Statement

Even though, Sri Lankan Personal Data Protection Act No. 9 of 2022 regulates the processing of personal data in the country, it does not explicitly outline a systematic approach for embedding privacy into technology design. As a result, how to adopt the PbD principles into the software development lifecycle (SDLC) is at software companies' discretion and no study has conducted to explore the current status of adoption of PbD into SDLC in Sri Lanka.

This study investigates the adoption of PbD in the Sri Lankan software industry. It explores the current state of PbD implementation in Sri Lankan software development, identifies the technical and organizational measures (TOM) required to integrate PbD, and examines how data privacy can be embedded into technology design from the earliest stages of SDLC. A qualitative research approach is employed, incorporating both primary and secondary data collection methods to comprehensively assess the landscape of PbD adoption in Sri Lanka.

1.2.1 Research Objectives

The primary objectives of this study are:

1. To explore the current status of the application of PbD in the Sri Lankan software development industry.
2. To describe the technical and organizational necessary for implementing PbD in software development processes in Sri Lanka.
3. To identify the business impact of incorporating data privacy through technology design.

1.2.2 Research Significance

This study addresses critical contextual and methodological gaps related to PbD adoption in Sri Lankan software development.

The identified contextual gap is Sri Lankan companies lacking a clear path to compliance in privacy data protection. While extensive research exists on data

protection and privacy regulations in global contexts, there is a lack of understanding regarding the adoption of PbD within Sri Lankan legal and technological frameworks (Jansen, 2022). The Personal Data Protection Act No. 9 of 2022 does not provide specific guidance on integrating privacy into technology design..

Previous research has explored topics such as data protection, privacy governance, and GDPR compliance. However, these studies do not offer insights into practical methodologies for embedding privacy into software development practices within the Sri Lankan context (Accounting Nest, n.d.). This study aims to bridge that methodological gap by identifying suitable methodologies and best practices tailored to Sri Lankan software companies.

By addressing these gaps, this research contributes to enhancing privacy practices in Sri Lanka's software industry, offering valuable insights into how companies can adopt PbD principles to build more secure, privacy-conscious applications.

1.2.3 Outline

This is the introductory chapter of the research. The researcher attempts to examine the background of the study in this chapter, including what PbD is and the legal structures available in Sri Lanka to protect the personal data of the individuals. The motivation of the research outlines what the researcher tries to achieve as the result of the study and clearly describes what has motivated the researcher to carry out the research. The objectives of the study outline what the researcher wants to achieve with the investigation. Examining previous studies and the issues that need to be addressed through the research helps the research problem examine the research gap. The significance of the study is discussed in terms of the grounds upon which the researcher bases that conclusion. This study also makes an effort to explain how the discovery will benefit later researchers. The limits of studies draw attention to their shortcomings.

CHAPTER 2

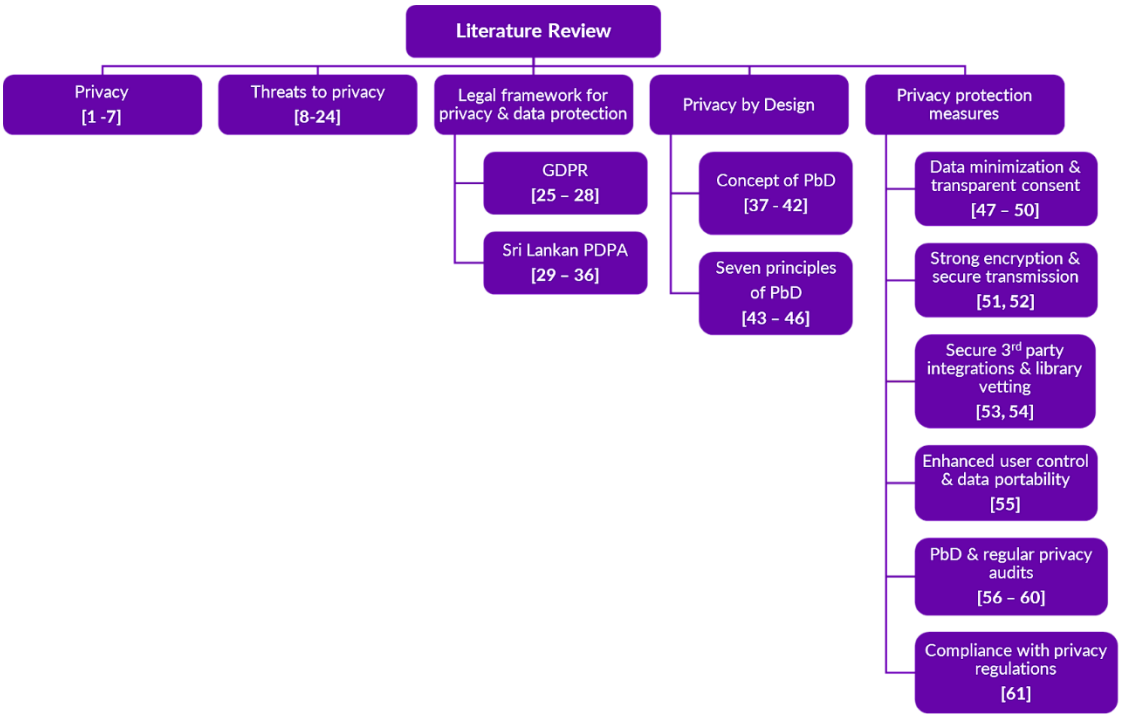
LITERATURE REVIEW

2.1 Introduction

As the digital landscape expands, privacy concerns have become a critical focus in software development within the IT industry. The exponential growth in data collection and processing has heightened the need for effective privacy practices to safeguard sensitive information. Ensuring privacy is no longer a reactive measure but a proactive strategy embedded throughout the software development lifecycle. This literature review explores key aspects of privacy in software development, including PbD, the General Data Protection Regulation (GDPR), and region-specific data protection laws such as Sri Lanka's Personal Data Protection Act. These frameworks provide insights into evolving practices and regulatory requirements shaping privacy protection in today's technological environment.

Figure 1

Literature Review Overview



2.2 Privacy

Businesses want a comprehensive data strategy that balances offense and defence in the right ways (Davenport, 2017). Defence entails reducing risks associated with data use, and offense entails leveraging technologies like predictive analytics to support business goals. Defence mandates that enterprises have risk policies to regulate the risks connected with the use of data, including privacy, in the same manner that they have risk policies for financial and other important assets (Hoepman, 2023).

Data privacy, sometimes also referred to as information privacy, is an area of data protection that deals with the proper handling of sensitive data, most notably personal data, but also other confidential data, such as certain financial data and intellectual property data, to meet regulatory requirements and protect the confidentiality and immutability of the data (SNIA, 2022).

The security and protection of personal data are only one aspect of data privacy. What matters most is how businesses are exploiting those personal data. Organizations must handle personal data in a moral and legal way. That can entail refraining from sending clients an overwhelming number of pointless SMS marketing messages, but it might also just entail refraining from disclosing personal information to third parties without the customer's agreement (Data Privacy Handbook a Starter Guide to Data Privacy Compliance, 2020).

Identification of private information during Internet transmission is one important concern with user privacy (Bednar et al., 2019). Although they may appear to be the same, data security and privacy are two distinct concepts. Security focuses increasingly on defending data against malicious attacks and the use of stolen data for financial gain (Bednar et al., 2019). Data privacy focuses on the usage and control of individual data, including measures like putting in place regulations to ensure that customers' personal information is being gathered, shared, and used in the proper ways (Jain et al., 2016).

Due to interactions between humans and robots that necessitate constant collection and processing of personal data, endangering the privacy of users, ensuring that the data collected is impervious to a privacy breach is one of the main concerns related to data collection (Bednar et al., 2019).

2.3 Threats to Privacy

The following section will discuss the critical areas such as regulations on privacy compliance, storage insecurities, data collection methods, user controlling aspects and dependencies on third part sources. Even though there are multitude of threats are present, one needs to have a conceptual understanding and a method of addressing of

the said aspects which will be critical for developing software that secured and complies with privacy fundamentals (Gellert, 2015).

Data collection has deep routed to the foundation of any modern software. Including in e-commerce platforms, social media platforms, health and wellness monitoring systems, data collection is widely applied by the developers to personalize the offering (Acquisti, Brandimarte and Loewenstein, 2015). However, the risk levels vary depending on the type of data gathered. In many cases the issue is the excess collection of personal data, going beyond the traditional requirement for the application performance. This level of increased data collection is leading to privacy risks as well as creating vulnerabilities in case of a data breach or an exposure occurs (Payton & Claypoole, 2023).

In many cases, data collection happens invisibly. This means the user is unaware of the collection and uses a "freemium" model which tracks the user activities without a general notification or electronic user agreement (EULA). In many cases, internet surfing patterns, location details and contact are commonly harvested which will potentially be used by developers to populate look-alike audiences. This issue not only put the user data sovereignty under threat, it also raises a possible ethical concern on the informed consent (Cofone, 2023). High privacy sensitive areas such as finance and healthcare collection of data such as financial transactions, financial patterns or medical records can post a greater threat to the both user and the developer (Hansen, Jensen and Rost, 2015).

Data storage and data transmission is a critical matter in software development. Once the data have been obtained, raw-data or processed information must be protected from internal and external threats (Hu and Sastry, 2016). Storing data in insecure platforms or facilities with weak encryptions can lead to unnecessary data breaches. In 2017, Equifax had a privacy breach where over 147 million people's data were exposed due to unpatched vulnerabilities and weak data encryption (Aguilera et al, 2020).

Even if the data is securely stored, data breach will be easy if the data remains in plaintext form. Furthermore, APIs with insecure encryptions will pose a significant threat to data privacy (Danezis et al, 2015). Since most modern applications are depending on third party APIs to enhance the speed and app performance such as payment processing, multi-app integration such as social media platforms, APIs are putting everything in to an easy yet critical junction. Weak or poorly designed APIs can expose the user data to malicious actors, especially when authentication and encryption are not properly implemented.

Third-party library usage and integration has become a common norm in modern day software development. Developers generally have frequently access libraries and Software Development Kits (SDKs) to fast track the development process without complicating the functionality of the app and without reinventing the wheel. In some cases, there have been scenarios where hackers have introduced vulnerabilities (Leenes, 2017). As for an example, advertising SDKs that are commonly found in mobile apps on tracking user behavior in many apps, carry a concern about the user

profiling and cross-app tracking. Depending on these third-party apps will allow data breaches and often share the collected information with external parties that can potentially cause a large-scale privacy violation. This issue gets even worse if the developers are unaware of the data collection extensions used by libraries (Zuboff, 2015).

Users possessing control over their personal data is a fundamental principle of privacy. Many of the commonly reported threats arise when the users are not allowed to take control over the information that are collected (Solove, 2013). Also, it should be the norm that the user should be able to control how their data is collected, informed how the data is stored and shared. In many cases, users are unable to delete the provided information when the application is deleted or unsubscribing from the service. Without the ability of removing the data that has been already shared, user loses control leaving the data vulnerable in case of a future misconduct or an attack. This issue magnifies when such information is left with companies without a proper privacy data policy or a purpose (Aguilera et al, 2020).

2.4 Legal Framework for Privacy and Data Protection

Laws and regulations on data protection around the world have been rapidly transformed to ensure greater protection and privacy for the personal data. With the introduction of GDPR many countries have adopted their own framework in accordance with that regulation (Huth, Clarke and Kumari, 2020). In Sri Lanka, Data Protection Act, No. 9 of 2022 is also created accordance with GDPR, focusing on rights to data subjects or individuals, strict conditions for consent, data access, data collection (ICTA, 2022).

2.4.1 GDPR

GDPR is a major advancement in data and privacy protection laws imposed by the European Union (EU) aiming at protecting individual data and granting them rights to privacy. The impact of GDPR not only applies to EU based organizations, but any organization that involves with processing the data of citizens of EU (Huth, Clarke and Kumari, 2020).

Figure 2

Fundamental Principles of GDPR

GDPR is based on 7 basic principles as indicated in the above framework, which are aimed to push organization to be responsible for the provision of maximum protection to individual privacy. The first principle of Lawfulness, Fairness and Transparency is the core principle which influence other principles. Lawfulness is concerned with having a legally valid reason for data collection (such as consent or legal obligation). In this case consent should be obtained without any sort of influence with the right to withdraw the consent at any time. Fairness is about informing an individual on the data collection without holding any information. This is critical to avoid any kind of deception or misinformation provided for individuals to manipulate them to consent. Transparency is the use of collected data only for the stated purpose (Bertram, Borrmann and Poddey, 2019).

The first principle directly influences the principles of purpose limitation and data minimization, which advocates for collecting data that is only relevant for the stated purpose and to collect minimum amount of data that adequate to cater the purpose. Storage limitation, demand the time period data being stored and deletion of data after the purpose has been served (Voigt and von dem Bussche, 2017). Data quality requires conducting checks and audits for data accuracy and removing the inaccurate data. Information security and Protection by design and default advocates to the having privacy and data security through the system design and also the privacy policies (Bertram, Borrmann and Poddey, 2019).

2.4.2 Sri Lankan Data Protection Law

Sri Lanka Personal Data Protection Act No. 09 of 2022 is implemented following the GDPR guidelines in order to safeguard personal information and encourage

development and innovation in the digital economy. The Act seeks to guarantee interoperability among systems for protecting personal data and to improve cross-border collaboration. It outlines safeguards for private and governmental organizations, including banks, telecom providers, hospitals, and government agencies, that hold personal data (ICTA, 2022).

A name, identity number, financial information, geographical information, or online identifiers are examples of personal data, according to the Personal Data Protection Act (PDPA), which defines personal data as any information that can be used to directly or indirectly identify a data subject. Whether alive or deceased, the data subject is a natural person to whom the personal information pertains and who can already be identified or identified using the information (Mahingoda, Harasgama and Jayamaha, 2024). A natural or legal person who determines the intended uses and methods of processing personal data is known as a data controller. A third party that follows the controller's orders is known as a data processor. Any action taken on personal data is considered processing, including gathering, storing, preserving, changing, retrieving, disclosing, transmitting, making available, erasing, destroying, consulting, aligning, combining, or performing logical or mathematical calculations (Madushani and Dharmaratne, 2022).

The Data Protection Act is a set of principles that entities handling personal data must adhere to. These principles include Lawfulness, Fairness, and Transparency, which require data to be processed lawfully, fairly, and transparently. Organizations must inform individuals about data collection purposes and obtain their consent when necessary. Personal data can only be collected for specific, legitimate purposes, and data minimization should be limited to the necessary amount (De Silva, 2022). Accuracy is crucial, and inaccuracies must be corrected or erased promptly. Storage should not exceed the required duration for the collected purposes. Finally, data must be processed securely, including protection against unauthorized or unlawful processing, loss, destruction, or damage (ICTA, 2022).

The Act mandates that data controllers must obtain explicit consent from individuals before collecting or processing their personal data, unless there is a legal obligation. A data subject's freely provided, explicit, informed, and undisputed consent is an evidence of their acceptance to the processing (Dissanayake, 2022). Data subjects have a number of rights under the Personal Data Protection Act (PDPA) to guarantee that their personal information is handled fairly. These rights include the ability to access their data, demand erasure if they feel the controller is processing their data in violation of their obligations, object to processing if it is in the public interest or if the controller is pursuing a legitimate interest, and withdraw consent if processing is based on consent (De Silva, 2022). Furthermore, in certain conditions, like automated decision-making, which impacts their rights to equality and nondiscrimination, the PDPA acknowledges data subjects' right to have decisions made by controllers reviewed. The exercise of this right, however, may be restricted by specific requirements, such as processing only with express consent or requiring a contract between the controller

and the data subject. In general, the PDPA seeks to strike a balance between controllers' and data subjects' interests (Fernando and Wickramasinghe, 2022).

The Act mandates data controllers and processors to ensure compliance with data security and prevent breaches. They must maintain records of processing activities and conduct Data Protection Impact Assessments (DPIAs) in cases where processing poses a high risk to individuals' rights and freedoms (Goswami, 2022). With the exception of the court, the act mandates the appointment of a data protection officer (DPO) in cases where the controller is a government ministry, department, or public enterprise as well as in cases where large amounts of data are processed. DPOs must be assigned to core processing activities that involve processing certain categories of personal data, monitoring data subjects on a regular basis, or processing that could jeopardize the rights of data subjects. In addition to advising controllers on compliance with the new regulation, including staff capacity building, impact assessments, and collaboration with data protection authorities, DPOs must be knowledgeable and skilled in personal data protection methods (Mahingoda, Harasgama and Jayamaha, 2024).

The Data Protection Act in Sri Lanka regulates cross-border data transfers, ensuring that these transfers occur only when adequate data protection measures are in place in the receiving country. This is crucial for multinational organizations and companies outsourcing data processing to other countries. The Data Protection Authority (DPA), an independent regulatory body, monitors compliance and enforces the law. The DPA can investigate complaints, conduct audits, and impose administrative fines on organizations violating the Act. Non-compliance can result in significant penalties, including fines and sanctions. The DPA can issue directives to rectify non-compliance and impose fines based on the severity of the breach (Fernando and Wickramasinghe, 2022).

2.5 Privacy by Design

2.5.1 Concept of PbD

PbD is a proactive approach that embeds privacy considerations into the entire lifecycle of a product or system, from its inception through to its deployment and maintenance. This framework aims to anticipate and prevent privacy breaches before they occur, rather than merely reacting to them. In the context of software development, PbD emphasizes the importance of integrating privacy features directly into the architecture and processes used to create IT systems, ensuring that privacy protection is not treated as an afterthought or add-on (Cavoukian, n.d).

The concept of PbD stems from the recognition that traditional privacy safeguards, such as regulatory compliance and user agreements, often fall short in addressing privacy challenges in today’s fast-paced digital environment (Parrilli, 2024). As systems become increasingly complex, the volume of personal data processed has grown, making it essential to adopt an approach that can address privacy risks at every

stage of the software development process. By incorporating PbD into software development, organizations can foster user trust, reduce the risk of data breaches, and ensure that they meet legal and ethical obligations regarding data protection (Bieker et al, 2016).

Moreover, PbD aligns with various global data protection regulations, such as the EU's GDPR which mandates data protection measures from the design phase of a system onward (Chattopadhyay and Berkovsky, 2021). For software developers, this means incorporating technical mechanisms, such as data minimization, encryption, and access controls, early in the design process. This approach not only strengthens privacy protections but also contributes to building more secure, resilient systems (Hansen, Jensen and Rost, 2015).

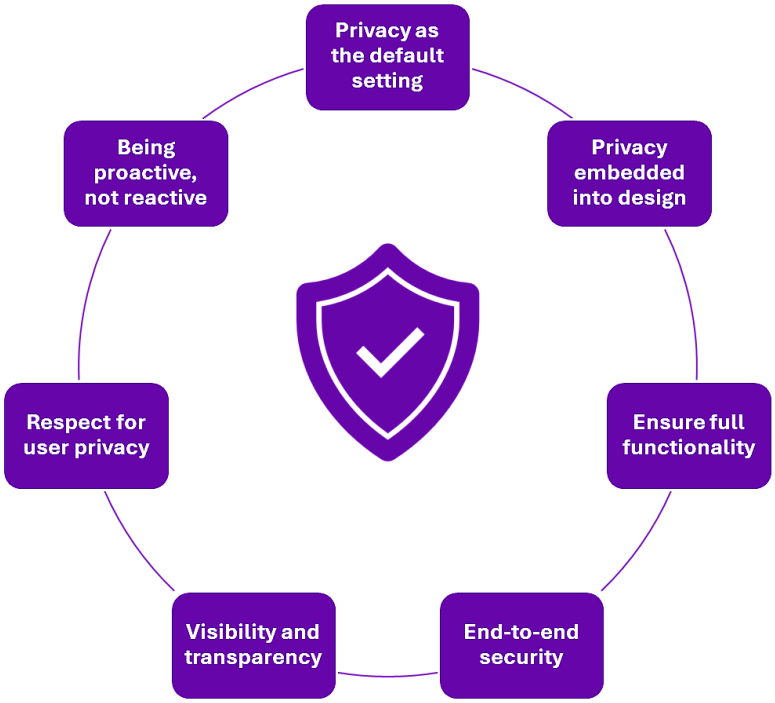
In essence, PbD shifts the focus from reactive measures to a more forward-looking, preventive strategy, enabling privacy and data protection to be central to the development process in the IT industry (Gurses and van Hoboken, 2020).

2.5.2 Seven Principles of PbD

PbD by Canadian Dr. Ann Cavoukian who is the mastermind behind these rules. This looks at safeguarding the information in the modern world (Cavoukian, n.d). As many people are using computers and mobile phone on a daily basis and are extremely dependent on them, it is important that information stays private and there are 7 aspects which he speaks that the information must be kept.

Figure 3

Seven Principles of PbD



Proactive, not Reactive; Preventative, not Remedial

As per Parrilli (2024), according to the first rule, it is important to have a futuristic consideration and thinking ahead. He highlights the importance of not waiting for the last minute to protect information, but to ensure be prepared to keep it safe. Likewise, this approach is all about being prepared before getting damaged for being late.

For an example in the case of building a house, it is important have the roof completed as soon as possible and not wait for the rainfall to complete the roof. Author insists that the privacy protection must work the same way where when companies are introducing new product lines and service approaches, it is extremely important that privacy concerns are addressed at all times (Schwartz, 2017).

Author further speaks about how a company such as a social media app developer should focus on privacy even before the app codes are built (Cronk, 2021). It states that questions such as how shall the user messages are kept private? How the photos can be secured and how to limit the access by 3rd parties to ensure the data platforms are consistent and uninterrupted. Companies who have addressed these questions at their beginning have been successful in reaching to the customers effectively. Such an approach is important to ensure the privacy is built in to the app at all times in different angles.

It is also important to note that Author states that it is important to keep lookout for new ways to protect privacy. Along with the technology changes, there could be many privacy risks that could loom and companies must ensure those aspects are covered or otherwise the products can fail in the blink of an eye.

Privacy as the Default Setting

According to the author, the second rule is about building the norms around privacy like in a case of a door that must be closed all times until there is a need arises for someone to open it but by default doors must be closed (Stallings, 2020).

When new products are innovated, it is important to have the personal information protected automatically and it should not be a case where the users have to put an extra effort safe guard their data and personal information (Stallings, 2020). Under this approach, author advises to collect the bare minimum personal information through a software, not sharing the information wide out open and using a strong mechanism to protect the personal identities at all times.

According to Rubinstein and Good, (2013), it further defines that when launching a new application, it should automatically be set to use the maximum privacy protection and privacy settings. Users should not be needed to navigate the software to increase the privacy protection. This approach helps people who are not tech-averse also to be well covered with privacy protection. This theory also applies to not only the individual based apps or software but the company-maintained software as well.

Author also recognizes the fact that this approach is going to make the app less personalized and it should strike a balance between which details should be collected and prioritize which data are utilized to provide a super experience (Gürses, Troncoso and Diaz, 2011).

Privacy embedded into Design

This principle mentions that privacy should be included in the core system or built in to the core product and not to be purchased or added as an extra off-the shelf feature. Author states that when creating new software and services, privacy must be considered at all steps including the data collection methodology, system design and coding and user interaction points.

In many cases, software and system carry an easy-to-understand form that explains how the data are used and gathered and allow the users to navigate the existing high-profile privacy settings. This method ensures that the privacy approach is not lapsed at any moment and is deeply rooted in to the core of the system. However, there are arguments and disagreements coming in to this method where the development cost of the system gets far too expensive and the development may be too complex for infant software companies. Furthermore, smaller software developers might find it difficult to balance privacy needs with the core needs due to the costing aspects of the development (Tamò-Larrieux, 2018).

Full Functionality (Positive Sum-not Zero-sum)

This principle strongly argues the matter that systems should be high in privacy and better at functionality. Developers must be capable of developing systems that are high in performance and be able to protect privacy at all costs. As for an example, an app might be 100% functional on a mobile device and should be equally encrypt the user data and must not share the personal information without prior approval of the user.

According to Colesky, Hoepman and Hillen, (2016), this principle pushes the developers to innovate creative and efficient approaches for the app development where the privacy is not lapsed when the system is performing 100%. It also allows marketers and business decision makers to push the product as a solution to existing opportunities. However, there are critics regarding this approach where in practical scenarios protecting privacy can limit the full potential of the software/system due to the limitations and limits at the personalization level. Software that are providing personalized content are mainly becoming the victim of this approach where the high security is limiting the personalized experience to the users.

End-to-End Security Full lifecycle protection

These principal advocates that the data or the privacy information must be protected from the time of collection until the data is no more needed or deleted. In order to facilitate this requirement, systems must have a strong encryption to protect data, secure paths who can control the access to the data, setup deletion protocols where companies decide that the data is no more needed and conduct regular inspection checks to ensure the privacy data stays secured at all times (Stallings, 2020).

The core objective of this approach is to prevent unauthorized access to data and protects against possible security threats. While this is seeming very important, there are parties that argue that this data protection technique can be extremely expensive and difficult to maintain mostly for smaller organizations. This approach in return can make the systems to be non-friendly and can be harder to adopt to provide a personalized experience.

Visibility and Transparency – Keep it Open

This principle encourages app developers to be clear and honest about how the personal information is used (Colesky, Hoepman & Hillen, 2016). Author states that this is as similar to using a glass-box than a dark box where user should be able have a clear idea about what is happening to the information that is collected.

In order to facilitate this approach, it is advisable to have a clear set of policies which are easy to understand. Also, inform the users about changes happening in how the data is used. Finally, let the users journey easy to navigate the user privacy settings. Author states that the openness allows the developer to build trust with the user. It also helps organizations to follow privacy regulations that require people about data use.

However, there are arguments that it will be a difficult task to explain complex data collection algorithms to users in lament terms. Also, if lament terms are used to communicate the said purpose, users are likely to get a wrong impression as they will not get the full picture of the data collection. Many argues that many users are not reading even 1% of the privacy agreements and thus, it is a pointless effort to keep the data policies open at all times (Cronk, 2021).

Respect for User Privacy – Keep it user-centric

Final principle states that protecting the privacy of the users must be the important goal of the app development process. Systems must be build in order to give control to the users to control their own data. This means allowing people to select the amount of data they need to share with app/software and seek the user permission before collecting such. Moreover, make it easy for users to stop sharing their personal information in case of a change of mind (Tamò-Larrieux, 2018).

This principal highlights the fact that privacy is a basic right of any user and the sharing of such information must be done at the user discretion. There are arguments that not all people require to toggle the amount they need control over and some parties argue that too many privacy controls might distract the user and at time can even confuse the user to the complexity of the enablement.

The above 7 principles of PbD intended to create a strong approach to protect the personal information. The guidelines provided to navigate how the technologies created and used allows companies to build trust with end-users about the services rendered through the software and abide to all the laws that can potentially apply.

However, it should be noted that putting these principles in place can be a challenging task as mentioned in previous situations as the complexity required in planning, costing and balancing the scope of the system.

2.6 Privacy Protection Measures

In the realm of software development, privacy threats are increasingly complex, stemming from issues such as excessive data collection, insecure storage, and third-party vulnerabilities. While these challenges are significant, robust solutions exist to mitigate privacy risks and enhance user trust. This essay will explore the most pressing privacy threats within software development and emphasize detailed solutions that developers and organizations can adopt to safeguard personal information.

2.6.1 Data Minimization and Transparent Consent

One of the most effective ways to mitigate privacy risks is through data minimization. This principle advocates for collecting only the data necessary to perform a specific function, reducing the volume of sensitive information that could be compromised (Alshammari and Simpson, 2021).

Limit data requests to only what is necessary for the application's core functionality. For example, if an application requires location data only for a specific feature, it should not continuously track the user’s location in the background. Frequent reviews of data collection policies ensure that unnecessary data collection practices are identified and removed. This is particularly important for applications that may initially collect more data than needed for potential future features (Joshi and Finin, 2019).

Clear consent mechanisms should be incorporated to inform users about data collection practices. Rather than relying on vague or hidden terms, developers should provide granular consent options, allowing users to choose which types of data they are comfortable sharing (Christin and Kerschbaum, 2020).

Transparency further improves user trust. By educating users about what data is being collected and how it will be used, developers enable informed consent. This can be achieved through concise and readable privacy policies, with pop-up dialogs offering clear explanations and options for users to accept or deny data collection (Cebula and Young, 2020).

2.6.2 Strong Encryption and Secure Transmission

Inadequate encryption and insecure data transmission pose serious privacy risks, particularly as cyberattacks become more sophisticated. Protecting data at every stage from collection to storage and transmission is critical.

End-to-end encryption should be a default practice for transmitting sensitive data. Transport Layer Security (TLS) ensures that data is securely transmitted between the

client and server, while encryption-at-rest (e.g., AES-256) safeguards data stored on servers or databases. Developers should also ensure secure session management using techniques like HTTP Strict Transport Security (HSTS), which forces the use of HTTPS for all communications between users and web applications (Karimi and Atallah, 2019).

Secure API design is essential, especially when interacting with third-party services. All APIs should require proper authentication (such as OAuth 2.0) and use encrypted communications to protect sensitive user data during transmission (Engelhardt and Maurer, 2020).

Regular encryption audits are necessary to maintain security over time, as cryptographic standards evolve. Developers should also rotate encryption keys periodically and implement key management best practices, ensuring that encryption keys are stored securely and separately from the encrypted data.

2.6.3 Secure Third-Party Integrations and Library Vetting

Many software applications rely heavily on third-party libraries, plugins, or SDKs (software development kits). While these dependencies improve development efficiency, they can introduce significant privacy vulnerabilities if not carefully vetted (Niu and Zhang, 2021).

Thorough vetting of third-party libraries is essential before integration. Developers should review the privacy policies and security practices of all external libraries, ensuring they adhere to stringent data protection standards. Libraries should be frequently updated to patch vulnerabilities and ensure compliance with evolving privacy regulations (Xue, Liu and Dong, 2020).

Developers should also prefer open-source libraries where possible. The transparency of open-source code allows security and privacy experts to audit the software and identify potential issues before they can be exploited.

If third-party SDKs are necessary (e.g., for advertising or analytics), ensure they offer clear data usage documentation and limit the scope of data collection. For instance, if an analytics SDK collects user data, its access should be restricted to anonymized data unless explicitly required and permitted by the user.

To maintain oversight, developers can implement sandboxing techniques, isolating third-party libraries and limiting their access to user data. By setting specific permissions, developers ensure that third-party components only interact with data required for their operation.

2.6.4 Enhanced User Control and Data Portability

A key principle in modern privacy regulation, such as GDPR, is the right of users to control their personal data. Allowing users to have full control over what data is collected, how it is used, and how long it is retained is central to improving trust and

reducing privacy risks.Granular privacy settings should be made available within applications, allowing users to decide exactly what data they wish to share. For instance, a social media app might allow users to control who can see their posts, what types of notifications they receive, and whether their location is tracked (Wong et al, 2020).

Implement data portability features that allow users to easily export their data in a machine-readable format. This gives users control over their data and allows them to move it to other services if desired.

Offer data deletion options that enable users to permanently erase their personal information. This should extend beyond simply deactivating an account and include the complete removal of associated data from all systems, including backups.

To ensure user trust, developers should communicate clearly about the impact of data deletion—such as the inability to recover an account after data is permanently erased. Providing self-service privacy dashboards within the application gives users a sense of empowerment over their own data.

2.6.5 PbD and Regular Privacy Audits

PbD is a proactive approach that integrates privacy considerations into the software development lifecycle from the very beginning. Rather than retrofitting privacy features, PbD encourages developers to embed privacy features at every stage of design and development (Stallings, 2020).

During the requirements gathering phase, privacy should be a core consideration. Developers should conduct Privacy Impact Assessments (PIAs) to identify potential privacy risks associated with new features or data collection practices. These assessments help in understanding where personal data may be exposed and inform the necessary safeguards to be implemented (Parrilli, 2024).

Developers should also adopt the principle of data minimization throughout the lifecycle of the software. Whenever personal data is collected, there should be a clear rationale and safeguards in place to ensure it is used only for its intended purpose (Gurses, Troncoso and Diaz, 2016).

Regular privacy audits should be conducted to ensure compliance with privacy regulations such as GDPR, CCPA, and HIPAA (Health Insurance Portability and Accountability Act). These audits help identify any emerging privacy risks or vulnerabilities in the system (Bertram, Borrmann and Poddey, 2019).

PbD also encourages the use of de-identification techniques such as anonymization or pseudonymization where appropriate. By stripping out personally identifiable information (PII) or replacing it with pseudonyms, developers can still analyze user data without exposing individual users to privacy risks (Tamò-Larrieux, 2018).

2.6.6 Compliance with Privacy Regulations

With global privacy regulations such as GDPR and CCPA, compliance is no longer optional—it's mandatory (Bertram, Borrmann and Poddey, 2019). Failure to adhere to these regulations can lead to hefty fines and loss of user trust.

Developers should implement systems that allow users to exercise their rights under privacy laws. For example, GDPR grants users the right to access, correct, or delete their data, while CCPA requires companies to provide transparent disclosures about data usage and sale.

Implement privacy-friendly default settings that comply with legal requirements. For example, GDPR mandates that users must provide explicit consent for data collection, particularly when dealing with sensitive data. Default settings should prioritize user privacy, such as disabling non-essential tracking unless the user opts in.

Establish cross-border data transfer safeguards. Applications handling international users must ensure that data transfers across borders comply with local data protection laws. For instance, under GDPR, data transferred outside of the EU must have the same level of protection as within the region.

Organizations should also appoint a Data Protection Officer (DPO) where applicable, to oversee data privacy strategies, ensure compliance with regulations, and act as the point of contact for regulatory bodies.

In conclusion, while privacy threats in software development are multifaceted, there are numerous solutions that developers can implement to mitigate these risks. Through practices like data minimization, strong encryption, secure third-party vetting, and PbD, developers can create secure software that respects user privacy. By empowering users with granular controls, offering transparent data practices, and ensuring compliance with privacy regulations, developers not only safeguard personal data but also build trust and loyalty among users. As privacy concerns grow in an increasingly data-driven world, adopting these proactive solutions is essential for both ethical and practical reasons.

2.7 Summary

The extensive literature review carried out in this chapter was able to gain a greater understanding of the Privacy. This especially includes numerous definitions, the legal perspectives both internationally and locally, privacy related threats and challenges, privacy protection measures as well as the PbD along with the 7 principles that guide the concept. Commonly privacy is more or less defined as the restriction of information to unauthorized or non-consented parties both as a measure of security and also as a right.

In the IT sectors, the privacy threats were found to be arising from data collection practices, data storage and transmission, over-dependence on third parties, insufficiency in user controls, lack of attention to privacy guidelines and weak data

protection laws. These threats were found to be highly detrimental the security of user data and confidence of users who rely on these platforms.

From the legal perspective, on the Privacy in the IT sector was found to be regulated by the GDPR and the PDPA, where the former dictates the international rules, while the latter dictates the rules related to companies within Sri Lanka. Both legal frameworks enforce accountability, transparency and more rights to users strengthening the privacy loopholes. A closer observation reveals that PDPA rules and guidelines are more or less based on the same guidelines of GDPR thus making the Data protection laws in Sri Lanka to be harmonized with GDPR.

In addition to the laws, PbD was identified as a concept that guides in a more comprehensive scale on how to ensure privacy from the design level. The aim is to make the privacy a core part of the system design and to make it a more proactive measure, thus placing greater importance on Privacy. In order to safeguard the level of privacy measures such as; Data encryption, anonymization, establishing access controls and adopting of secure software development protocols were found to be critical.

The literature review provides an important pre-text for the study of privacy in the Sri Lankan IT sector by providing a comprehensive scope of definitions, threats, controls measures, concepts and legal perspectives, which can be evaluated with the findings to determine the effectiveness of the practices followed in Sri Lanka for privacy.

CHAPTER 3

RESEARCH METHODOLOGY

The research methodology section further discusses what the research problem is, the research method, data collection method, how the population and sample are selected and the process of data collection.

3.1 Research Problem

The everyday reality of various social phenomena and examining significant topics as they are really applied, aid in providing answers to huge questions. A research problem can be described as the gap or issues in the existing knowledge aiming to address in the research (McCombes, 2019).

The research problem addressed through this research is investigating PbD in the context of software development in Sri Lanka. The research problem is focused around exploring the existing implementation and the adoption of Privacy by Design principles in the software industry of Sri Lanka. The unavailability of precise guidelines on applying data privacy through technology design despite the existence of Personal Data Protection Act No 9 of 2022 is a major issue prevailing when regulating the processing of personal data.

The researcher asserts that the investigation will offer a thorough grasp of the aspects such as;

• How aware are the software companies in Sri Lanka about the adoption of Privacy by Design?

The study includes the evaluation of whether the companies are proactively integrating data privacy into the software development processes or if the software development companies consider about the privacy concerns only after the development is complete.

• What are the privacy practices followed by the software companies in Sri Lanka?

The research will focus on analysing the existing privacy and security policies and data protection measures practiced by the Sri Lankan software companies to safeguard personal data during the processing.

• What are the challenges faced by Sri Lankan software development companies while adopting PbD?

The identification of technical, legal, and organizational barriers that affect when integrating data privacy in software development.

• How data privacy can be integrated in the early stages of the software development lifecycle?

This can be achieved by exploring the privacy-aware design methodologies and privacy-conscious software architectures.

• What are the Technical and Organizational Measures (TOM) proposed by these organizations to implement PbD effectively?

The technological and privacy frameworks along with employee training and organizational policies are included here.

3.2 Research Method

There are three main types of research methods that can be used for collection of data namely; quantitative approach, qualitative Approach and mixed methods approach. For investigating PbD in the context of software development in Sri Lanka, the qualitative approach has been chosen. Under this approach, non-numerical data is collected and analysed in order to understand the concepts, opinions, or experiences is the main aim of carrying out a qualitative data analysis. This approach can be used in order to come into better conclusions by gaining new insights about data when carrying out the research (Booth, 2018). The primary reason for choosing qualitative approach is that the researcher wants in-depth answers to the questions that cannot easily be put into numbers. The researcher believes that human experience on this topic can be understood thoroughly.

3.3 Data Collection

To identify solutions to research problems, to respond to inquiries, to assess results, and to predict trends and probabilities, data collecting is the process of obtaining, measuring, and analysing precise data from a range of pertinent sources. Making educated business decisions, ensuring quality control, and maintaining the integrity of research all depend on accurate data collecting.

Data collection of this study involved both Primary data and Secondary data. Primary data is mainly used in core data analysis, while the secondary data is used in the supplementary roles such as gathering literature and background information.

For the purpose of collecting Primary data, the adopted method is Interviews. Interview is a direct interaction between the researcher and the respondent in order to build up conversations relevant to a certain topic and collect information is the key aim of holding interviews. An interview can be held in-person, over the phone and through video conferencing. Interviews can be structured which implies that the questions are predefined, semi-structured as it allows flexibility and unstructured as it can be more conversational (Simplilearn, 2021). The researcher has chosen interviews as the primary data collection method in order to investigate the PbD in the context of software development in Sri Lanka, because researcher wants to collect in-depth and concise data about the topic.

Secondary data has been collected using various methods such as; Peer-reviewed journal articles, credible books and online articles, government databases and statistics, as well as industry reports. All the secondary data sources will be publicly available data.

3.4 Population and Sample Selection

The precise group from whom the researcher will gather data is referred to as a sample. Every time, the sample size is smaller than the population. For this research, since selecting all the software development companies functioning in Sri Lanka is impractical. Therefore, a sample was drawn from with consideration to the below characteristics.

- Individual should be working in a medium-scaled software development company in Sri Lanka.
- The organization should have employee base between 50-250.
- Individual should either be the owner or a director of the company, or should at least hold a position of senior lead if an employee.
- Individuals must have Privacy handling as a key part of their job role.
- The individual should have a minimum of 2 years of experience in privacy handling.

The sampling technique used for the research is Purposive sampling. Purposive sampling popularly known as judgmental or selective sampling is a non-probability sampling technique where the researcher uses his own judgement in order to choose the participants for the research (Alchemer, 2021). The researcher has selected purposive sampling as the sampling technique since a particular subset of people should be accessed as all the chosen participants fit for carrying out the research. Under this sampling strategy there were 7 individuals selected for the study.

3.5 Interviewee Profiles and Thematic Analysis Process

There were seven interviewees involved in the interviews carried out to collect data for the analysis. The while all seven of them were found to be meeting the sample criteria, their profiles are given below for further understanding.

Table 1

Interviewee Profiles

Interviewee #	Profile Summary
1 – Team Lead (Software Development)	Experience: 6–7 years in the software development industry. Domain Expertise: ERP and enterprise software integrations.

	Current Role: Leads the B2B communication product team at a product-based company. Key Responsibilities: Oversees product enhancements and releases, manages budgets for SaaS and self-hostable software, attends client meetings, and reports team progress to management. Company Focus: Provides both self-hostable and SaaS/cloud-based B2B software solutions.
2 – Senior Information Security analyst	Experience: Nearly 6 years in cybersecurity. Domain Expertise: Security compliance and standards (PCI DSS, ISO 27001/20000, NIST). Current Roles: Senior Information Security Analyst at a leading Sri Lankan cybersecurity firm and visiting lecturer in cybersecurity law. Key Responsibilities: Conducts compliance reviews, vulnerability assessments, penetration testing, and security code reviews, primarily for banking, telco, and software firms. Company Focus: Cybersecurity consulting and assessments.
3 – DevOps Engineer	Experience: Over 5 years in software development. Domain Expertise: Telecommunications sector, CI/CD automation, infrastructure management. Current Role: DevOps Engineer for customer and retailer support applications. Key Responsibilities: Oversees deployments, manages CI/CD pipelines, monitors systems, and collaborates with developers for seamless integration and stability. Company Focus: Telco-based customer and retailer support solutions.
4 – Senior Software Engineer	Experience: 10+ years in commercial software development. Domain Expertise: React, cloud architectures, customer engagement platforms. Current Role: Senior Software Engineer. Key Responsibilities: Develops and maintains application code, ensures quality through testing, collaborates in sprint planning, and manages CI/CD pipelines and documentation. Company Focus: AI-driven CRM and loyalty solutions for personalized consumer experiences.

5 – Business Analyst	Experience: Nearly 5 years as a Business Analyst in Sri Lanka's IT sector. Domain Expertise: CRM and integrated enterprise software for local and international clients. Current Role: Business Analyst (has also taken on senior software engineering responsibilities). Key Responsibilities: Gathers requirements, contributes to planning, manages code quality, CI/CD, and documentation. Company Focus: Broad software solutions, with emphasis on CRM and integrated systems.
6 – Tech Entrepreneur and Product Designer	Experience: Founder and product designer for several leading Sri Lankan software products. Domain Expertise: Consumer apps, B2B platforms, and educational tech. Current Roles: Founder and Product/UX Designer for "Helakuru", "PayHere", and "Hapan". Key Responsibilities: Leads product vision, UX design, and overall strategy across multiple platforms. Company Focus: Diverse software targeting consumer (Helakuru), business (PayHere), and children's (Hapan) segments.
7 – Legal Consultant (Tech and Privacy Law)	Experience: Over 10 years in law, including government, telco, and private consultancy. Domain Expertise: Data protection, privacy, and digital rights. Current Role: Independent legal consultant specializing in tech law. Key Responsibilities: Advises companies on data protection frameworks, privacy regulations, and regulatory compliance; contributed to drafting Sri Lanka's Personal Data Protection Act. Company Focus: Legal advisory services for tech companies and digital platforms.

Note: Author based on Analysis results

The insight generation was performed by thematic analysis technique for the data gathered from the interviews, however the main themes of the study were pre-determined as Privacy, Sri Lanka Data Protection Law, PbD and Embedding Privacy. Under the theme the sub level themes and codes were identified from the data and then linked towards the main themes. Under this process, the were 16 sub themes that were

identified under the 4 main themes, providing a rich content of findings on Privacy in Software Development in Sri Lankan IT Industry.

3.6 Process of Data Collection

Upon selecting the sample, the participants were interviewed by the researcher in order to collect precise and concise information related to the research topic. The researcher conducted the interviews through video conferencing tools as it is convenient in terms of time and effort. There were 7 interviews conducted from various Sri Lankan based professionals in the software development companies as the primary data collection method. The researcher prepared interview guides and protocols along with the relevant questions that answered all the areas covering the research topic. The questions asked ultimately answered the research objectives while being clear and unbiased. The researcher chose to conduct the interviews by using the structured method where the participants are provided with a predefined set of questions so that they can prepare for the interviews beforehand in order to answer them precisely. The questions are then tested on a test interviewee so that any issues or ambiguities can be identified before actually conducting the interviews. Furthermore, the researcher collected the data with the help of trustworthy library based published resources in order to collect more information to support the topic. The data collected from both primary and secondary methodologies were stored securely for further analysis using a suitable qualitative analysis technique.

3.7 Theoretical Framework

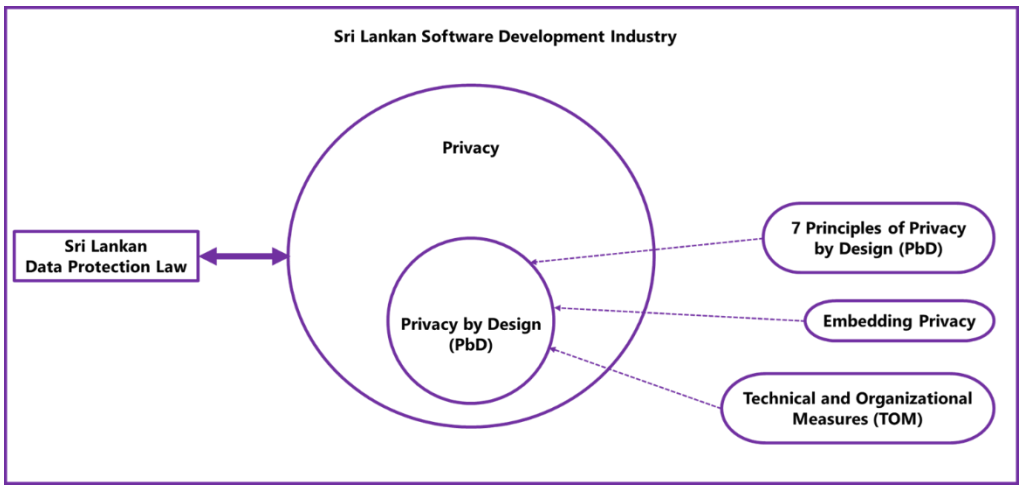
A theoretical framework is a collection of related ideas, precepts, and premises that serves as a framework and road map for comprehending a certain occurrence or conducting study in a particular area.

In essence, it serves as a framework or lens for researchers to examine and understand data, make observations, and reach conclusions. The social sciences, natural sciences, and humanities are just a few academic areas that frequently use theoretical frameworks. They offer a conceptual framework that aids in thought organization and the formulation of research questions or hypotheses.

By creating a theoretical framework, researchers can pinpoint the crucial elements, connections, and mechanisms at work in their investigation.

Figure 4

Theoretical Framework of the Study



The theoretical framework for PbD in the Sri Lankan Software industry is shown in the above figure. PbD is a subset of the concept privacy. The goal of the idea and methodology known as "PbD" in the software industry is to incorporate privacy considerations into the planning and creation of software systems from the very beginning. Its focus on integrating privacy safeguards into the overall design and architecture of software programs, products, and services makes it a subset of privacy (Jayashankar, 2020).

CHAPTER 4

DATA ANALYSIS AND DISCUSSION

4.1 Introduction

The purpose of this chapter is to provide the interpretations of the data analysis carried out based on the interviews done. These interpretations will provide a deeper understanding on how the IT sector of Sri Lanka defines privacy and their awareness of the local data protection law and PbD as a concept along with how privacy is embedded in their experience with the industry. This chapter will also include a discussion that will reflect on the findings and compare them with the literature insights to determine the extent to which the findings draw similarities or differences with the literature.

4.2 General Themes in Privacy by Design

4.2.1 Theme 1 - Privacy Theme

4.2.1.1 Definition of Privacy

Under the Privacy theme, one of the sub themes identified was the "Definition of Privacy". This theme was emerged as the interviewees explained in great detail regarding what they understand as the concept of Privacy. In these explanations, it was evident that there are multiple of perspectives taken by them to define the concept of privacy; Privacy as a right, Privacy as a legal requirement and Privacy as a technical process. The multi-dimensional nature to the concept given by the interviewees gives privacy a rich perspective and also indicates there thorough understanding of the concept.

A significant number of definitions on privacy was also defined as a right of an individual. According to these definitions privacy is about safeguarding a person's right to set boundaries on what kind of information they wish to reveal and what kind of information that they wish to keep in secret. This can be illustrated by the following statement; *"In my opinion, privacy is one's right to safeguard and control their personal information. Data protection measures are used to protect personal data by ensuring confidentiality and privacy"*.

The interviewees who focused on the legal perspective of privacy emphasized privacy as commitment to the privacy conditions agreed through a legal contract and to respect the all the law and practices of a country related to privacy. This can be illustrated by the following statement; *"privacy should also respect the legal requirements which comes from both through privacy agreements and the general law"*.

The least discussed perspective of privacy is the technical perspective of privacy, as stated by one interviewee as; *"Privacy is also about the steps taken to ensure the Privacy of person, such as implementing access controls, or putting limitations for the type of data that will be collected"*. In this perspective, the idea is to establish controls and restrictions to what outside parties can access regarding one's information and creating authorizations when needed.

4.2.1.2 Privacy Requirement

The second sub theme identified under the privacy theme was the "Privacy Requirements". Theme was emerged from the insights where the interviewees explained about the challenges they faced when ensuring privacy in their software development projects. As a result of those challenges they able to explain the kind of skills and knowledge that is required in a person when it comes establishing privacy. When looking at the opinions of the interviewees it was evident that the Privacy requirements were expressed in terms of Academic Knowledge, Prior experience of the individuals in establishing privacy and the ability to be in touch with the evolving landscape of Privacy. This sub theme gives a rich insight on what a person should be having within themselves if they are to be handling privacy related matter when developing software in the Sri Lankan IT industry.

Academic Knowledge in Privacy was heavily emphasized by two of the interviewees, making it one an important requirement for person to ensure privacy when developing software. It was highlighted how the academic and professional knowledge gained helped them to be more aware and knowledgeable on how to ensure privacy. It was also emphasized how lack of sound academic background create challenges for individuals in the beginning of their careers as an IT professional involved software development, as stated by one interviewee; *"in the start of my career I had a lot of difficulties since I was not academically qualified. But some of my peers who had degrees, had a better understanding than me since they have learnt them in their universities"*.

Prior experience with privacy establishment was another privacy requirement and also the one that was mostly emphasized by the interviewees. It was evident from the data that, as heavily experienced professional they currently have little to no difficulties or challenges, which was result of the accumulated experience over the years, as stated by one interviewee; *"Difficulties are part and partial of this job. But with experience I have lesser difficulties, since I now I know what to do in most of the challenges"*.

The third requirement highlighted is the ability to become updated with the evolving privacy landscape. Respondents who favored this argument, critical pointed out that this is an ability that cannot be gained from neither academic knowledge nor experience, but the constant research and learning about the incidents that happen in this privacy landscape. This is because, new threats, new law and new technologies emerge continuously which caused the prior knowledge and experience to become non-relevant.

4.2.1.3 Privacy Implementation in Software Development

The third sub theme identified under the privacy theme was the "Privacy Implementation in Software Development". Theme was emerged from the insights where the interviewees explained about the how the privacy protection practices are implemented in their workplaces when carrying out software development projects. This allowed for an exploration of variety of ways how companies in Sri Lanka is enforcing privacy in their software developments. When looking at the opinions of the interviewees it was evident that the Privacy Implementation in Software Development was discussed in four main areas of; Policies, Mechanisms, Principles and Guidance. This also reveals the status of the Sri Lanka IT industry on their level of commitment to enforce privacy.

Privacy Policies were emphasized by three interviewees as an important part of implementing privacy. Policies define which data will be disclosed and will be accessed by whom thus it gives a scope and an understanding to both parties.

Mechanisms were the mostly emphasized measure which includes; establishing access controls, data encryption and pseudonymization, granting special access in critical cases as well as using of different cloud servers for different clients. The following statement illustrates this sentiment; *"We take privacy very seriously and limit access to data through our customer or retailer support applications as much as possible. Users can only see the minimum data needed to fulfill their job, reducing risk of unauthorized access to information".* As the most discussed measure on implementing privacy, this prove to be the most critical towards enforcing privacy.

Principles are also highlighted as important since it provides direction for the companies the basic foundation for establishing privacy. Among these Principle of Least Privilege and Need to know basis are critical towards ensuring only the needed data are collected and only the needed data are being accessed.

Guidance even through least mentioned measure, is still found to be critical on preparing both employees of the development company and the users of the client firm on how privacy can be safeguarded on a personal level by following the proper practices instructed to them.

Table 2

Thematic Summary for Privacy Theme

Main Theme	Sub themes	Codes
Privacy	Privacy Definition	Privacy as a right, Privacy as a legal requirement, Privacy as a technical process
	Privacy Requirements	Academic Knowledge, Prior Experience, Updating and evolving

	Privacy Implementation in Software Development	Privacy Policies, Privacy Mechanisms, Privacy Principles, Guidance

Note: Author based on Analysis results

4.3 Context-Specific Themes in the Sri Lankan Software Sector

4.3.1 Theme 2 – Sri Lankan Data Protection Law

4.3.1.1 Personal Data Protection Act

Under the SDPL theme, one of the sub themes identified was the "Personal Data Protection Act". This sub theme is critical to understand the level of awareness of the IT professionals regarding the law and their knowledge regarding the specific aspects of the law on Privacy.

It was evident that most of the interviewees have a good enough understanding of the PDPA and the main points of it. There was a clear understanding among the interviewees that PDPA enabled greater privacy rights and data security for the users such as the right to not give consent for obtaining data or withdraw the consent, limiting of data collection and especially imposing regulations when there are involvement of cross-border transactions and activities. Another important point highlighted was the intention of PDPA to align the privacy and user protection standards of Sri Lanka with the global standards such GDPR. One interviewee made a critical point where PDPA defines role for both Data Controller and Data Processor (*"When it comes to the obligations of the Data Controller the act mentions a few special points like the consent of the end user"*).

Despite the high level of awareness portrayed by most of the interviewees, there were two of them who does not have sufficient awareness regarding the law. As emphasized by one of those two candidates; *"I'm somewhat familiar with the Personal Data Protection Act, No. 9 of 2022 since I'm more close to the customer information. From what I've read, the act is designed to safeguard the personal data of Sri Lankan citizens"* which show case the limited awareness, while the other interviewees were clear about their lack of awareness of the law or its content even though being in the IT field for many years.

4.3.1.2 Technical and Organization Measures that enforce SDPL

The second sub theme identified under the SDPL theme was the "Technical and Organization Measures that enforce SDPL". Theme was emerged from the insights where the interviewees explained about the kind of organizational and technical measures taken by the organization they are employed currently and employed in the past, Through this sub theme, it was able to discover a range of technical and organizational measures put in place to ensure privacy and how these technical and organization measures compare against data encryption and pseudonymization, which

are the recommended technical and organizational measures by the SDPL. Therefore, it provides an understanding on how the technical and organizational measures have impacted as a result of the SDPL.

The interviewees were able to provide a rich range of technical and organizational measures where the most commonly mentioned measure was the access controls such as the two-factor authentication and planning for privacy right form the software designing stage. Additionally, there was mentioning about carrying out routine audits to ensure the privacy measures are implemented as planned. These measures are illustrated in the below statement; *"Well, I am not the best to comment on this, but to my knowledge things like data protection measures from unauthorized access, measures of encrypting, defined practices for coding are important. I believe audits also play a key role"*. Even though highlighted least, there are two other measures discussed which are the Defined Coding practices and assessment by data controllers on the technical and organizational measures of related third party data processors as emphasized by one interviewee as; *controllers need to assess the TOMs of any third party they outsource data processing to. This requirement should be part of the due diligence process during RFP assessments.*

Apart from the above measures, the most important two measures discussed was the data encryption and pseudonymization, since these two measures were the recommended two measures by the SDPL. Regarding these two measure there were different opinions expressed by the interviewees. Firstly, out of the two measures data encryption was comparably highlighted more making its use to be more frequent, as emphasized by one interviewees as; *"Since AWS is our main cloud service provider, all Amazon S3 buckets have encryption configured by default, and all new objects uploaded to Amazon S3 are automatically encrypted by using server-side encryption with Amazon as keys. We have implemented those features into our software when we are providing our solutions to such customers"*. However, Pseudonymization particularly mentioned by some interviewees particularly in certain cases such as in the telecommunication industry as emphasized by one interviewee as; *"We also used pseudonymization to keep customer data anonymous during development and testing, making sure we didn't expose real data unnecessarily"*. Despite the recommendation in the law, there was critical opinion by one interviewee highlighting that data encryption and pseudonymization not being widely used, where other measures such as access controls are used more due to the cost and complexity.

Despite the numerous viewpoints gathered, 2 interviewees demonstrated their lack of understanding regarding the technical and organizational measures implemented by their organization with regards to privacy. Even though it was claimed that they were aware, there was no understanding to explain any kind of specific measures. As emphasized by one of the the interviewees; *"Yes, I'm aware of, but I don't have that much knowledge about the specific measures to comment in a detailed manner"* is evident statement of their lack of understanding, even though these participants are employees in the IT sector who have a direct involvement in the development of Software.

Table 3

Thematic Summary for SDPL

Main Theme	Sub themes	Codes
SDPL	Personal Data Protection Act	Privacy rights, Right to consent, Limiting of data collection, Regulations on cross-border transactions and activities, Role of Data Controller and Data Processor,
	Technical and Organizational measures	Access Controls, Planning for privacy at design, Defined Coding practices, Assessment by data controllers on the technical and organizational measures, Data encryption, pseudonymization

Note: Author based on Analysis results

4.3.2 Theme 3 – Privacy by Design

4.3.2.1 Understanding of PbD

The first sub theme identified under the PbD theme was the "Understanding of PbD". Theme was emerged from the insights where the interviewees explained about their familiarity of the concept of PbD. The insights from the transcripts revealed different levels of familiarity with the concept and also different perspectives towards the concept of PbD.

Among the interviewees, despite two interviewees were found to be less familiar with PbD, most them was found to be highly familiar with the concept and showed good understanding on what the concept means. The common definition to the concept was having Privacy as a core part of the design rather than as an additional requirement as emphasized by an interviewee; *"It's about making privacy a key part of IT system design from the very beginning. This means that privacy isn't just added on later but is built into the system right from the start"*.

It was evident from the insights that this concept is being understood by as a Proactive approach, rather than a reactive approach. This is because the concept pushes privacy in to the core of the system design to add measures in order to prevent privacy breaches from happening.

Another important point highlighted by one interviewee was the conflict arises with the actual business requirements of the client, when practicing PbD. The main argument against it was found to be detrimental impact it has on business performance and innovation as emphasized by the interviewee; "*one of the biggest criticisms of having privacy regulations, I mean, this is something even the Sri Lankan, when we were drafting it, the level against the introduction of such a law was that this is going to inhibit innovation and it's going to be a costly affair and whatnot*".

It was also revealed by one interviewee that companies tend to focus more on putting PbD into practice when they experienced Privacy related incident in past projects as illustrated by the following extract; *"Previously we didn't practice like that but after the incident we changed to incorporate privacy starting from the design level"*.

4.3.2.2 Foundation principles of PbD

The second sub theme identified under the PbD theme is the "Foundation principles of PbD". This theme was a direct emergence, as it was questioned by the interviewees directly on their awareness and understanding of the 7 Principles of PbD.

In terms of the awareness and understanding of the 7 Principles of PbD, it was evident that all the participants were aware that there are 7 foundation principles related to PbD, however, only few of them could recall all seven of the principles. This indicates that there is a good level of awareness, yet differing level when it comes to thorough understanding of it.

Among the 7 principles, most interviewees were found to be thoroughly knowledgeable on two of the principles namely; Principle 1 - Proactive not Reactive, Principle 2 – Privacy as a default setting and Principle 7 – Respect for user Privacy. This also provides an indication that these are the principles that are mostly applied in practice, as the IT professionals could recall and explain them with ease when it is used in their projects. This was further emphasized that one interviewee illustrated in the following statement; *"Actually, in the framework there are seven principles that needed to be considered when implementing privacy from the design perspective. But the reality all seven principles are not being considered. But the principle of privacy by default is commonly used and practiced"*.

4.3.2.3 Application of Privacy as a Default of the Design

The third sub theme identified under the PbD theme is the "Privacy as a Default of the Design". This theme was a direct emergence, as it was questioned by the interviewees to recall on the application of Privacy as a Default in their implementations. It was evident from the insights that all the interviewees could recall this feature being applied in their past projects.

Most interviews emphasized Privacy as a Default of the design was implemented through developing user-centric software, private data storages and high level of access controls, where only a specified person is authorized to access data as mentioned by an interviewee; *"Sure, our software solutions are user centric, and all user data is stored in a private location which is accessible only by the specific user through a default dashboard login, and until he or she decides to expose it to any other systems by creating integrations or any entry points into set storage location. So, it's by default, only accessible to the particular user"*. One interviewee highlighted on case by case review for data access to prevent any person from exploiting data access loopholes in categorization.

It was also highly emphasized by several interviewees that limiting the collection of data as another way towards implementing privacy as a default as illustrated by the

following statement of an interviewee; *"let's look at an online credit card payment. As the data processor we are receiving certain data of the credit card, for example the name of the card holder, expiry date and so on. Just because we receive all those data, we are not storing all that. We are storing the data which is crucially needed for business purposes only. This is how we follow data minimization in our default setting"*. One interviewee further emphasized on questioning or demanding for justifications for collection of piece data as a mechanism to minimize data collection.

Table 4

Thematic Summary for PbD Theme

Main Theme	Sub themes	Codes
PbD	Understanding of PbD	Privacy as a design element, Proactive nature, Conflict between privacy and business need.
	Foundational Principle of PbD	Proactive not Reactive, Privacy as a default setting, Respect for user Privacy
	Application of Privacy as a default in the Design	User-centric storage, data limitation, purpose of collection.

Note: Author based on Analysis results

4.3.3 Theme 4 – Embedding Privacy

4.3.3.1 SDLC stage of Privacy consideration

The first sub theme identified under the Embedding Privacy theme is the "SDLC stage of Privacy consideration". This theme provides a clear understanding on what is the stage in SDLC, where the Privacy is largely considered. The stage of the cycle it was considered is also an indicator on the level of importance given to privacy by the Software developers.

From the insights of interviewees, it was evident that all the software developers are now considering privacy in the early stages, as all the interviewees mentioned stage of considered as *"from the beginning"*, *"from the design stage itself"* or *"initial stages"*, which indicating a high level of importance given for privacy. It was also further emphasized by one interviewees that starting from the initial stage, privacy should be concern across all stages.

There were two reasons highlighted by two interviewees for this tendency, one the privacy related incidents in the past projects making them understand the important of

considering privacy right from the design stage. The other reason is the difficulty to change or alter any privacy settings at later stages as emphasized by an interviewee; *"Different stakeholders, such as marketing and sales teams, may push for extensive data collection, while legal and regulatory teams will be more cautious. It's important for me to address these privacy concerns early on because incorporating them later can be challenging"*.

4.3.3.2 Design Practices

The second sub theme identified under the Embedding Privacy theme is the "Design Strategies". From the interviewees insights this identified as separate segment from the previously discussed privacy related practices and technical and organizational measurements, since the strategies are set to decide how the previously discussed practices and measures should be implemented. Under this theme there was a diverse mix of opinions from the interviewees.

One of the strategies mentioned is to have User level of boundaries in design diagrams that defined the access level for each user. Privacy impact assessments are also mentioned by one interviewee as a where the potential for privacy breach at every part of the system is assessed in the early stages. Two other strategies mentioned by other interviewees; Customer journey mapping and the Employment of security and privacy team can also be taken synonymous with Privacy Impact Assessments, since these two are more or less approaches for privacy impact assessments. Another interviewee, highlighted Involvement of all stakeholders as a critical strategy for integrating PbD principles, where it allows for a comprehensive understanding privacy requirements.

Despite the different strategies coined by the interviewees, it was evident that the core of the strategies shares high level of similarity with each other.

4.3.3.3 Privacy Trade-off

The third sub theme identified under the Embedding Privacy theme is the "Privacy Trade-off". This theme provides an understanding on between privacy and functionality, or else the cost of integrating privacy into the systems.

Among the opinion on whether there is a trade-off between privacy and functionality of a system, most of the interviewees agreed on the existence of a trade-off, clearly emphasizing that one cannot increase the both ends at the same time. As explained by an interviewee; *"Certainly, there may be a trade-off between privacy integration and essential features. Strong encryption and stringent access controls, for example, may occasionally cause system performance to lag or increase user experience complexity. When privacy controls are completely integrated, this may result in slower data processing times or a more complicated user interface in the applications we build"*.

As per the interviewees, the trade-off could go both ways depending on the situation. Interviewees that highlighted situations where functionality is prioritized over privacy indicated it as a result of lack of attention for privacy from client until the latter stages, which makes integrating all the privacy requirements to be challenging. Furthermore, another interviewee emphasized the need for simplistic, user-friendly software also

drives for more scarification of privacy in order to make it understandable a less tech-savvy person. On the other hand, interviewees have highlighted that the priority becomes shifted towards Privacy, when there are past incidents that occurred due to inadequate consideration for privacy.

Contrary to the above opinion, one interviewee emphasized that the trade-off is merely a perception and both privacy and functionality could co-exist. It was strongly argued that the co-existence is possible to when the privacy is considered right at the early stages; *"By integrating privacy from the start, we can create systems that are both functional and secure. It may require more effort initially, but it builds trust with users and ensures compliance with regulations"*.

4.3.3.4 Responsibility for Privacy

The next sub theme identified under the Embedding Privacy theme is the "Responsibility for Privacy". This theme explores the parties in a Software development company that is responsible for the embedding of Privacy.

As per the interviewee insights the common understanding that can be gained is that Responsibility of ensuring privacy is a shared or collective responsibility as illustrated by the following statement; *"Responsibility-wise, I can't pinpoint one role and say that this role is primarily responsible for embedding privacy into the project"*. As a result, the responsibility cannot be passed on to a specific person or team.

Even though not directly mentioned of a collective responsibility, interviewees who have pointed out certain roles as responsible for privacy also had a lot of diversity. Out of the interviewees Product Owner, technical leaders, development team, lead engineers, legal and compliance team, security team and Data protection officers are mentioned as parties responsible for the Privacy. This number of roles mentioned could also be a further indication that the responsibility is shared rather than individual or team centric.

Responsibility despite being collective, it was highlighted that some roles carry more weight of it according to the situation as illustrated by the flowing statement; *"Privacy is a collective responsibility. But the extent of responsibility differs in different stages. When making a framework for privacy, the legal teams bear responsibilities. But imagine if a specified privacy element is not in the final delivery, then the development team is more responsible"*.

4.3.3.5 Stakeholder Collaboration

Stakeholder Collaboration is also identified as a critical sub theme under the main theme of Embedding Privacy. Stakeholder Collaboration allows for the exploration of how stakeholders related to a software development project is involved towards establishing the privacy of that development. The findings indicate a mix perspective on who would be the main stakeholders that would be collaborated.

Under stakeholder collaboration, a significant number of interviewees highlighted customer as the main collaborating stakeholder. Since they are the main user of the software, interviewees have argued that their requirements should be given

prominence. As highlighted by one interviewee; *"Often privacy requirements or concerns are bought in by the customers themselves. We usually listen to their requirement over others because they are ultimately using the software"*.

Another noticeably highlighted stakeholder is the legal team. With the laws and regulations related to privacy is becoming increased, it is emphasized that the legal team has greater role to play as a collaborator.

Another emphasized perspective is that privacy establishment as a collaboration of many stakeholders together. In this perspective no stakeholder is highlighted to be important over others, and every involved stakeholder will provide their input. As highlighted by one interviewee; *"Like I told you before, making privacy a part of the software is a team effort. Security Consultants are not the only ones to be held responsible, but also legal teams, developers, marketing team and clients as well"*.

Apart from the above, there were also mentioning about Industry players through their standards set on privacy and the development team as key collaborators in Privacy.

4.3.3.6 Knowledge and Skills

The another sub theme identified under the Embedding Privacy theme is the "Knowledge and Skills". This theme explores the measures taken by the companies in the Sri Lanka IT industry to ensure the talent with right knowledge and skills in place in order to implement PbD in the software that are being developed. The findings indicate different mix of measures taken by the industry to develop the talent. Under this theme there were two different sets of measures that can be identified; Talent acquisition measures and Talent development measures.

The mostly highlighted measures out of the two measures by the interviewees were talent development measures. Under talent development the main emphasized measures were trainings which was seen as the key towards developing the knowledge and skills of the employees on Privacy and the Privacy related principles. This can be illustrated by the following statement; *"Our company ensures that the team is well-equipped to implement PbD by providing specific training on data protection and privacy principles"*.

The second key measure under talent development is the knowledge sharing which is seen as critical towards making everyone in the organization to be updated with the latest events and changes with regards to privacy. This can be illustrated by the following statement; *"To keep ourselves up to date with the emerging technologies, security practices and legal aspects, we have a weekly meeting like a knowledge sharing session where one person from the team will pick a topic and do a presentation to the entire team on the selected topic or the area. The intention of this session is to encourage continuous learning"*.

Apart from the key talent development measures workshops, online courses and certifications, self-learning as well as guidance were also highlighted by certain interviewees as talent development measures.

Some of the other measures highlighted by the interviewees can be identified as talent acquisition measures. The two measures highlighted under this type was having thorough assessments for hiring, in order to acquire high quality talent and to employ highly specialized employees to key positions as emphasized by following statement; *"The Security Engineers and the Consultants are specialized in Information Security discipline"*.

Despite the various measures mentioned, it is critical to note that one of the interviewees highlighted that there are no such specific measures to have the talent required to ensure privacy, other learning privacy through experience.

4.3.3.7 Privacy Impact

Privacy Impact is also identified as a critical sub theme under the main theme of Embedding Privacy. Privacy Impact allows for the exploration of how the integration of PbD would impact the Software development companies.

Under Privacy Impact theme, most of the interviewees emphasized the negative business impact due to not having the proper privacy mechanisms and measures in place. The negative impact of these incidents mentioned by the interviewees include; reputational damages, market share drops and share price drop which are critical negative business impacts. As emphasized by one interviewee; *"I can recall one of the famous incidents, there was an iCloud data privacy breach a couple of years ago, which had a significant impact on the stock values of Apple and iCloud market share. I believe the impact might have been much lesser if the proper privacy and data segregation mechanisms were in place and if they have considered privacy in the early stage of the project"*. It was also mentioned that these incident bring negative impact to both the client firm and the developer.

The positive impact of privacy measures is highlighted in two ways. One of the ways is the prevention of privacy issues in the current projects, as a result of the learnings through the mistakes committed in the past. As highlighted, a company is able to position better in as a software developer through improved privacy. The other ways discovery of the superiority of their one's privacy measures, through an incident happened due to the weak privacy measures of competitor. As stated by one of the interviewees; *"Privacy related incident comes by surprise. So I cannot clearly say that we made this particular privacy improvement, so it prevented a particular incident. But if we get to know that a particular incident occurred in a product developed by some other company. We can assess our privacy mechanisms and check whether it could happen to us as well. If we find out that our privacy mechanisms are strong and such an incident would not happen, now that is a point where we know how our mechanisms have prevented a bad privacy incident"*.

4.3.3.8 Competitive Advantage

The final sub theme identified under the Embedding Privacy theme is the "competitive advantage". This theme provides an understanding on how software development

companies in Sri Lanka is able to gain a competitive advantage by embedding privacy in to the technical design.

Most of the interviewees highlighted that by being able to embed privacy to design, it would allow development companies to gain a competitive advantage as a "trusted" software developer. As a privacy issues are more likely to emerge, not experiencing such issues in their systems creates the impression that the developer can be trusted. This can be illustrated by the following statement; *"I believe embedding privacy into technology design can indeed offer a competitive advantage. For example, if our applications for customer and retailer support feature advanced privacy controls by default, it builds trust with users. This can be a significant selling point"*.

Apart from trust, one interviewee highlighted the competitive advantage as a Safe and Secure software developer. It was argued that high level of emphasis towards privacy right from the design stage will create the assumption in the client mind that the software and system are safe and secure, which make them confident with the developer.

Another point of competitive advantage pointed out by an interviewee is to be a software solutions provider with "no trade-off". This is based on the argument that privacy and functionality can be balanced when privacy is applied from the initial levels.

Table 5

Thematic Summary for Embedding Privacy Theme

Main Theme	Sub themes	Codes
Embedding Privacy	SDLC	Consideration in Initial stage, importance of privacy in the initial stage, ease of configuration, consideration across all stages.
	Design Practices	User level of boundaries, Privacy impact assessments, Customer journey mapping, Employment of security and privacy team, Stakeholder involvement
	Privacy trade-off	existence of a trade-off, functionality over privacy, privacy over functionality, co-existence
	Responsibility for Privacy	Collective responsibility, Situationally differing responsibility, Development team, Product Owners
	Stakeholder Collaborations	Customer, Legal team, Industry players, Multiple stakeholders

	Knowledge and Skills	Talent development, Talent acquisition, Privacy trainings, knowledge sharing, workshops, self-learning, hiring assessments, employment of high value personnel
	Privacy Impact	Negative Impact, Positive Impact
	Competitive Advantage	Trust, Secured, Safe and high performing

Note: Author based on Analysis results

4.4 Discussion of Findings

4.4.1 Privacy Theme

The data analysis findings and the literature reveal a multi-dimensional understanding of privacy. Findings defined privacy through various lenses primarily as a right, a legal requirement, and a technical process. Most emphasized privacy as protecting sensitive personal and confidential information, aligning with the literature's focus on safeguarding personal data from unauthorized access (SNIA, 2022). Additionally, the legal aspect of privacy, highlighted by interviewees, resonates with the literature's emphasis on the importance of adhering to data privacy regulations (Jain et al., 2016).

A notable contrast exists regarding the technical perspective of privacy. While findings emphasized it minimally, the literature provides a more expansive discussion, particularly regarding the distinction between data security and privacy (Porambage et al., 2016; Bednar et al., 2019). There is a common agreement on the necessity of moral and legal handling of personal data, with the literature further stressing the role of businesses in responsibly leveraging data while respecting individual rights.

The analysis on privacy requirements for Sri Lankan software developers reveals a unique finding, as there was no evident literature directly addressing this topic. The data highlights three key competencies: academic knowledge, prior experience, and the ability to stay updated with the evolving privacy landscape. While academic knowledge provides essential theoretical foundations, prior experience helps professionals overcome privacy-related challenges. However, staying updated with emerging privacy threats, laws, and technologies was emphasized as a critical skill, requiring continuous learning. In over the highlights the importance of the importance of education, experience, and adaptability as a combination to ensure privacy in software development.

4.4.2 SDPL Theme

The data analysis findings and the literature both emphasize the importance of technical and organizational measures (TOMs) for ensuring data privacy. Findings reveal the access controls like two-factor authentication and incorporating privacy early in software design, aligning with the literature's focus on access restrictions and authentication mechanisms (Anderson, 2016). Routine audits and defined coding practices were highlighted in the analysis as additional methods, similar to the literature's emphasis on creating a secure environment for data processing through policies and employee training (William, 2019). However, as a TOM findings focus on assessing third-party data processors during due diligence. Even though it was less emphasized, it links with the literature's discussion by emphasizing accountability in data outsourcing.

The comparison between the data analysis and literature highlights a mix of awareness and gaps in understanding regarding SDPL among IT professionals. The analysis shows that most interviewees had a good grasp of the Personal Data Protection Act (PDPA), recognizing key aspects such as consent, data collection limits, cross-border regulations, and alignment with global standards like GDPR. This aligns with the literature's discussion of the PDPA as a framework aimed at strengthening privacy rights. However, while the literature emphasizes the existence of older laws like the Computer Crimes Act and Electronic Transactions Act. These laws offer only partial data protection, focusing more on unauthorized access and electronic transactions rather than comprehensive privacy measures. The literature also notes the limited scope of existing laws, contrasting with findings regarding the PDPA as a step toward modernized, global standards of privacy. The lack of awareness on the PDPA by some of the IT professionals despite their experience, reflects the need for further education on privacy laws as they evolve in Sri Lanka.

The data analysis and literature reveal both alignment and divergence regarding privacy measures like data encryption and pseudonymization. Findings emphasized data encryption as a more frequently used method, consistent with the literature's description of encryption as a widely adopted technique to secure data by making it unreadable without decryption keys (Cloudflare, 2022). However, pseudonymization, although recommended by the SDPL similar to Data encryption, is used in industries like telecommunications, but to a lesser extent when all industries are considered. The literature supports its role in enhancing privacy (James, 2020), yet the interviews suggest that its complexity and cost hinder wider adoption, with access controls often favored instead.

4.4.3 PbD Theme

The comparison between the data analysis and literature shows alignment on the concept of PbD. Both sources highlight it as a proactive approach, embedding privacy into system design from the outset rather than as a reactive, afterthought response to breaches (Varun, 2023). Interviewees also emphasized this proactive nature, seeing

privacy as integral to design, which mirrors the literature's description of integrating privacy into the core architecture (Jayashankar, 2020). However, the interview findings add a practical perspective, noting challenges like conflicts with business requirements and a tendency for companies to adopt PbD only after experiencing privacy incidents, which expands the literature's focus on proactive adoption.

With regards to the 7 principles of PbD, the data analysis findings indicate awareness on the 7 principles, despite many not being able to recall of them. Comparably the literature provides a highly descriptive explanation on each concept (Carbide, 2023; Cavoukian, 2006). It would be understandable though being industry experts, that they are not thorough with all the principles, since people tend to remember them if they are applied practically in a consistent basis. This has been the reason why most of them were able to explain 3 of the principles better.

The data analysis on Privacy as a Default of the Design presents unique insights that extend beyond the theoretical definition found in literature. While literature outlines this principle as an automatic privacy safeguard, the interviewees provided practical applications of it in their projects, emphasizing user-centric design, private data storage, and stringent access controls. The focus on limiting data collection and demanding justifications for collecting personal data is a notable practical approach that was not widely discussed in existing literature. This makes the finding distinctive, as it highlights how privacy is operationalized in real-world software development, especially in the Sri Lankan IT industry.

4.4.4 Embedding Privacy

The "Embedding Privacy" theme in the research uncovers several unique findings, as these insights are largely derived from real-world practices and experiences of IT professionals in Sri Lanka's software development industry. There is limited literature addressing the practical implications of embedding privacy within the SDLC (SDLC) or exploring the detailed strategies used by professionals in this field. Therefore, the insights gathered from the interviewees provide valuable, original contributions to understanding how privacy is operationalized and prioritized in software development.

First critical insight is the stag of SDLC where the privacy is being considered, which shows a notable shift towards prioritizing privacy from the earliest stages of software development unlike traditional practices where privacy was often an afterthought. This reflects a proactive and preventive approach to privacy, rather than a reactive measure. The rationale for this shift is the past incidents of privacy breaches and the difficulty of making privacy-related changes later in the development cycle pushing the focus on privacy as early as possible in the SDLC. This shift also underscores the growing importance of privacy in the software industry, which is not deeply covered in existing academic discussions.

The Design Strategies of privacy include user-level boundaries in design diagrams, Privacy Impact Assessments, customer journey mapping, and the employment of dedicated security and privacy teams. These strategies provide a structured approach

to privacy that goes beyond simple technical measures, diverging from traditional literature, which often isolates privacy into distinct technical controls.

Another important finding is the trade-off between privacy and functionality, where enhancing privacy might compromise some aspects of functionality. An alternative perspective argued that both privacy and functionality can co-exist if privacy is integrated from the early stages. This perspective is particularly significant, as it challenges the traditional notion of a zero-sum game between privacy and performance.

Findings also provided a diverse perspective on the Responsibility for Privacy which mainly argued collective responsibility approach to privacy within software development companies. Which included product owners, development teams, legal teams, and data protection officers. This indicates a shared, organization-wide commitment to privacy, which is becoming more ingrained in organizational culture, rather than a specific department's responsibility. The collaboration of stakeholders in the privacy setting such as customers, legal teams, and industry players further cements the notion of privacy as a collective responsibility and effort. This aligns with the increasing complexity of privacy regulations and the need for legal compliance, which is becoming a vital part of software development. The mention of industry standards set by other players also indicates that privacy is being shaped by external forces beyond the control of individual companies.

With regards to ensuring Knowledge and Skills needed to enable privacy in development projects, findings revealed various talent development and acquisition measures such as training, workshops, strict hiring assessment and certifications. The focus on talent development and acquisition also reveals the importance of building a privacy-conscious workforce that can handle the evolving challenges of privacy regulations and technology.

Findings on Privacy Impact reveals positive business implications of embedding privacy and negative implications on not properly embedding privacy. Negative implications included reputational damage and loss of market share due to privacy breaches, while the positive consequences included increased reliability, trust and confidence. These positive implications can also translate into a Competitive Advantage providing a competitive edge by positioning companies as trustworthy and secure providers.

CHAPTER 5

RECOMMENDATIONS AND CONCLUSION

5.1 Recommended Actions

Software development teams should prioritize embedding privacy requirements at the initial design stage. This involves mapping personal data flows and ensuring minimal data collection by default. By incorporating privacy considerations early, developers can avoid costly redesigns later and ensure that privacy measures do not compromise the user experience. This proactive approach ensures that data privacy is built into the foundation of the product, rather than being an afterthought, which can significantly reduce the risk of privacy breaches later in the software lifecycle.

The research highlights varying perspectives on privacy, ranging from it being a legal right, to a technical process, to a personal boundary. Organizations should prioritize educating their teams about the multifaceted nature of privacy. While legal compliance is crucial, it is equally important to understand privacy as a human right and as a set of technical controls. Developing comprehensive training programs that integrate these perspectives will help ensure that teams have a holistic understanding of privacy. By doing so, IT professionals can approach privacy more thoughtfully, balancing legal, ethical, and technical dimensions in software design and development.

The findings show that privacy is a shared responsibility involving product owners, developers, legal teams, and even clients, hence companies should foster cross-functional collaboration to ensure that privacy is addressed comprehensively. Legal teams can provide insights into evolving privacy laws, while technical teams implement the necessary controls. Clients, as end-users, should also be involved in the process to ensure their privacy concerns are addressed. Establishing dedicated privacy teams or committees, comprising stakeholders from various departments, can ensure that privacy remains a core focus throughout the project lifecycle.

While privacy policies and mechanisms are important, fostering a culture of privacy within organizations is equally essential. Employees and clients should receive guidance on how to handle data securely and responsibly. Companies could implement regular training sessions that focus on practical privacy practices, not only for technical teams but also for non-technical staff and end-users. This guidance should be clear, actionable, and context-specific, helping employees at all levels understand their role in safeguarding privacy. By embedding privacy-centric behaviour within the organizational culture, companies can ensure compliance and mitigate risks at every stage of software development.

One of the key findings is the importance of academic knowledge in understanding privacy principles. having a solid academic background from the beginning provides an easy way learn about privacy rather than trial and error. Companies should

encourage their employees to pursue professional certifications and academic programs related to privacy, data protection laws, and cybersecurity. Additionally, as privacy threats and laws are rapidly evolving, companies must create a culture of continuous learning.

The research shows that prior experience in establishing privacy protocols is essential for overcoming challenges in software development. Senior developers and IT professionals with extensive experience in privacy should be encouraged to share their insights and practical knowledge with less experienced team members. Companies could establish mentorship programs where seasoned professionals provide guidance on privacy implementation in real-world projects. By fostering a knowledge-sharing environment, the organization ensures that younger professionals learn from the practical challenges encountered by experienced individuals, thus improving their ability to address privacy concerns more effectively.

Regular privacy training sessions are crucial to keep teams informed about the latest privacy laws, regulations, and best practices. Training should emphasize secure coding practices, personal data handling, and privacy impact assessments. This ensures that all team members, from developers to project managers, have a strong understanding of privacy-by-design principles and are equipped to apply them effectively in their day-to-day work. Ongoing education will also help teams remain agile in the face of changing regulatory requirements and emerging privacy risks.

5.2 Limitations of the Research

While this qualitative study on privacy in software development within the Sri Lankan IT industry provides valuable insights, several limitations should be acknowledged. These limitations may have affected the depth, generalizability, and comprehensiveness of the findings.

One of the key limitations of this study is the relatively small sample size. Data was collected from only seven IT professionals, which may not be sufficient to capture the full spectrum of views and experiences related to privacy in software development within the broader Sri Lankan IT industry. While qualitative research often focuses on in-depth exploration rather than large samples, the limited number of participants may constrain the diversity of perspectives. For instance, the study may not fully account for variations in privacy concerns and practices across different sectors, company sizes, or types of software development projects (e.g., web development, mobile app development, or enterprise solutions). As a result, the findings may not be generalizable to the entire IT workforce in Sri Lanka.

The study is also geographically confined to the Sri Lankan IT industry, which has its own unique socio-economic, cultural, and regulatory environment. While this provides valuable context-specific insights, it limits the applicability of the findings to other regions or countries with different legal frameworks, cultural attitudes towards

privacy, and industry practices. For example Sri Lankan Privacy Law, may not be as deeply ingrained in the Sri Lankan IT sector, in the same way as how GDPR or CCPA, influence software development in other parts of the world. This regional specificity means that the study's conclusions may not be directly applicable to global software development practices or industries operating under stricter privacy laws.

Another limitation is the in participant selection, since the sample consisted of seven professionals, their personal experiences, roles, and levels of expertise may have shaped the findings. If these individuals were selected from a narrow range of companies, roles, or backgrounds, the study may unintentionally reflect the perspectives of a specific subset of the industry rather than a more balanced view. For instance, if the participants were predominantly senior professionals, the insights may reflect high-level privacy concerns rather than operational or technical challenges faced by mid-level developers. Similarly, if the professionals were drawn from organizations with well-established privacy policies, the study may not capture the struggles of smaller companies or startups with fewer resources to address privacy issues.

Finally, the study was conducted within a specific time frame, which might have limited the ability to capture evolving or emerging privacy concerns in software development. The fast-paced nature of the IT industry means that privacy practices and technologies are constantly evolving. New regulations, technologies, or privacy breaches could shift the industry's focus, meaning that findings based on the current state of privacy concerns may not be fully relevant in the near future. The dynamic nature of the subject means that ongoing research and continuous observation are necessary to capture a more comprehensive and up-to-date understanding of privacy in software development.

5.3 Achievement of the Objectives

Data analysis identified 16 sub themes under the 4 main themes. Though a main theme cannot be fully dedicated to a particular objective the sub themes can be clearly linked to particular objectives. As shown in the below table all the set 3 objective of the study has been covered by at least 2 or more sub themes providing an adequate cover up for all objectives.

Table 6

Achievement of the Objectives

Main theme	Subtheme	Objectives Covered
Privacy	Definition of Privacy	Generic Findings
	Privacy Requirement	Generic Findings

	Privacy Implementation	Generic Findings
SDPL	Personal Data Protection Act	Objective 1
	Technical and Organizational measures	Objective 2
PbD	Understanding of PbD	Objective 1
	Foundational Principle of PbD	Objective 1
	Application of Privacy as a default in the Design	Objective 2
Embedding Privacy	SDLC	Objective 1 & 2
	Design Practices	Objective 2
	Privacy trade-off	Objective 2
	Responsibility for Privacy	Objective 2
	Stakeholder Collaborations	Objective 2
	Knowledge and Skills	Objective 2
	Privacy Impact	Objective 3
	Competitive Advantage	Objective 3

References

Accounting Nest | RESEARCH-Methodological research gap: definition, identification and examples. (n.d.). Accounting Nest. Retrieved May 1, 2023, from https://www.accountingnest.com/articles/research/methodological-research-gap#:~:text=Methodological%20research%20gap%20is%20the

Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015) Privacy and human behavior in the age of information. Science, 347(6221), pp.509-514.

Aguilera, T., Fereidooni, H., Gruschka, N. & Sadeghi, A.R. (2020) Improving privacy and data protection in e-Health through private Blockchain. International Journal of Privacy and Health Information Management, 8(1), pp.21-41.

Alchemer. (2021). Purposive Sampling 101 | Alchemer Blog. Alchemer. https://www.alchemer.com/resources/blog/purposive-sampling-101/

Alshammari, M. & Simpson, A. (2021) Towards principled security engineering for privacy: A manifesto for security by design. Journal of Information Security and Applications, 58.

Bednar, K., Spiekermann, S., & Langheinrich, M. (2019). Engineering Privacy by Design: Are engineers ready to live up to the challenge? The Information Society, 35(3), 122–142. https://doi.org/10.1080/01972243.2019.1583296

Bertram, L., Borrmann, A. & Poddey, M. (2019) GDPR-compliant software design for cloud-based Building Information Modelling applications. Journal of Cloud Computing, 8(1), pp.1-13.

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H. & Rost, M. (2016) A process for data protection impact assessment under the European General Data Protection Regulation. Privacy Technologies and Policy, 9857, pp.21-37.

Booth, D. (2018). LibGuides: Research Methods: What are research methods? Libguides.newcastle.edu.au. https://libguides.newcastle.edu.au/researchmethods#:~:text=Research%20methods%20are%20the%20strategies

Cavoukian, A (n.d). Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Available at: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf [Accessed: 15-03-2025].

Cebula, J. J. & Young, L. R. (2020) Privacy risk analysis in software systems. IEEE Security & Privacy, 18(1), pp.31-40.

Chattopadhyay, S. & Berkovsky, S. (2021) Privacy-preserving data analytics: A survey on data privacy in machine learning. ACM Computing Surveys, 54(8), pp.1-36.

Cloudflare. (2022). What is Encryption? | Types of Encryption | Cloudflare. Cloudflare. https://www.cloudflare.com/learning/ssl/what-is-encryption/

Cofone, I. (2023). The Privacy Fallacy: Harm and Power in the Information Economy. (n.p.): Cambridge University Press.

Colesky, M., Hoepman, J.H. & Hillen, C. (2016) A Critical Analysis of Privacy Design Strategies. In: 2016 IEEE Security and Privacy Workshops. San Jose: IEEE, pp.33-40.

Cronk, R. J. (2021). Strategic Privacy by Design, Second Edition. United States: International Association of Privacy Professionals.

Danezis, G. et al. (2015) Privacy and data protection by design: from policy to engineering. European Union Agency for Network and Information Security.

Data Privacy Handbook A starter guide to data privacy compliance. (2020). https://www.pwc.com/m1/en/services/assurance/risk-assurance/documents/data-privacy-egypt-what-you-need-know-en.pdf

Davenport, T. H. (2017). What's Your Data Strategy? Harvard Business Review. Available at: https://hbr.org/webinar/2017/04/whats-your-data-strategy

De Silva, C. J. (2022) Privacy and data protection: Understanding Sri Lanka's new legal landscape. Journal of South Asian Law and Policy, 8(1), pp.55-73.

Dissanayake, R. (2022) The future of privacy and data protection in Sri Lanka: Exploring the new Personal Data Protection Act. International Journal of Information Policy, 12(2), pp.45-59.

Engelhardt, S. & Maurer, U. (2020) Secure and privacy-preserving online protocols. Proceedings of the IEEE, 108(4), pp.593-614.

Fernando, J. & Wickramasinghe, S. (2022) Sri Lanka Personal Data Protection Legislation – An Overview. SSRN.

Gellert, R. (2015) Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. International Data Privacy Law, 5(1), pp.3-19.

Goswami, S. (2022) Sri Lanka Data Protection Act: How Companies Must Comply. Bank Info Security. Avaialble at: https://www.bankinfosecurity.asia/sri-lanka-data-protection-act-how-companies-must-comply-a-20255 [Accessed: 20-09-2024].

Gurses, S. & van Hoboken, J. (2020) Privacy after the agile turn: Moving from value-sensitive design to critical privacy engineering. New Media & Society, 22(9), pp.1650-1675.

Gurses, S., Troncoso, C. & Diaz, C. (2016) Engineering privacy by design revisited. Computers, Privacy & Data Protection (CPDP) Conference, pp.3-29.

Hansen, M., Jensen, M. & Rost, M. (2015) Protection goals for privacy engineering. In: 2015 IEEE Security and Privacy Workshops, pp.159-166.

Hoepman, J. (2023). Privacy Is Hard and Seven Other Myths: Achieving Privacy Through Careful Design. United States: MIT Press.

Hu, H. & Sastry, S. (2016) A study on mobile information leakage and its countermeasures. IEEE Security & Privacy, 14(1), pp.34-43.

Huth, D., Clarke, N. & Kumari, J. (2020) Privacy in the GDPR era: Comparing perceptions from the UK and India. Journal of Information Security and Applications.

ICTA (2022) PERSONAL DATA PROTECTION ACT NO: 09 OF 2022. ICTA. Available at: https://www.icta.lk/icta-assets/uploads/2022/08/Article-Personal-Data-Protection-Act-Updates-April-2022-1.pdf [Accessed: 20-09-2024].

intersoft consulting services AG | Data protection and IT. (2018). Intersoft Consulting Services AG. https://www.intersoft-consulting.de/en/

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: a technological perspective and review. Journal of Big Data, 3(1). https://doi.org/10.1186/s40537-016-0059-y

Jansen, D. (2022, October 31). What Is A Research Gap (With Examples). Grad Coach. https://gradcoach.com/research-gap/#:~:text=The%20Contextual%20Gap

Joshi, A. & Finin, T. (2019) Attribute-based encryption for privacy-preserving access control in the cloud. Future Generation Computer Systems, 95, pp.92-103.

Karimi, B. & Atallah, M. (2019) Protecting the privacy of users in location-based services. IEEE Transactions on Dependable and Secure Computing, 16(2), pp.308-320.

Leenes, R., van Brakel, R., Gutwirth, S. & De Hert, P. (2017) Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues. Law, Innovation and Technology, 9(1), pp.1-44.

Madushani, M. S. & Dharmaratne, T. R. (2022) Privacy and data protection law in Sri Lanka: A comparative analysis with GDPR. Sri Lanka Journal of Legal Studies, 4(1), pp.45-60.

Mahingoda, C., Harasgama, K. & Jayamaha, S. (2024) The Implications and Implementation of Sri Lanka's Data Protection Act: Safeguarding Privacy in the Digital Age. 7th National Conference on Digitalization and Sustainability.

McCombes, S. (2019, April 15). How to Define a Research Problem | Ideas and Examples. Scribbr. https://www.scribbr.com/research-process/research-problem/

Niu, X. & Zhang, S. (2021) Privacy-preserving outsourcing for secure data processing in cloud computing. Future Generation Computer Systems, 117, pp.103-115.

Paasche, T.F. & Klauser, F.R. (2015). Surveillance and Privacy, Geography of. International Encyclopedia of the Social & Behavioral Sciences, [online] pp.727–732. doi:https://doi.org/10.1016/b978-0-08-097086-8.72124-6.

PARLIAMENT OF SRI LANKA. (2022). PERSONAL DATA PROTECTION ACT, No. 9 OF 2022 [Review of PERSONAL DATA PROTECTION ACT, No. 9 OF 2022].

Parrilli, D. M. (2024). Informational Privacy for Service Design: An Ethical Framework for Designing Privacy-Oriented Services. Switzerland: Springer.

Payton, T & Claypoole, T. (2023). Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family. United States: Rowman & Littlefield.

Schwartz, A. (2017). Digital Privacy at the U.S. Border: Protecting the Data On Your Devices. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/wp/digital-privacy-us-border-2017.

Simplilearn. (2021). What is data collection: methods, types, tools, and techniques. Simplilearn. https://www.simplilearn.com/what-is-data-collection-article

SNIA. (2022). What is Data Privacy? | SNIA. Www.snia.org. https://www.snia.org/education/what-is-data-privacy

Stallings, W. (2020). Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices. United Kingdom: Addison-Wesley.

Tamò-Larrieux, A. (2018). Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things. Germany: Springer International Publishing.

Voigt, P. & von dem Bussche, A. (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. In: Springer International Publishing, pp. 1-11.

Wagh, S. (2022). Research guides: Public health research guide: Primary & secondary data definitions. Researchguides.ben.edu. https://researchguides.ben.edu/c.php?g=282050&p=4036581#:~:text=Primary%20data%20refers%20to%20the

Wong, R.C. et al. (2020) Big data privacy: Challenges and techniques for data anonymization and de-identification. IEEE Access, 8, pp.186162-186192. DOI: 10.1109/ACCESS.2020.3030121.

Xue, M., Liu, J. & Dong, W. (2020) Achieving enhanced privacy in federated learning with differential privacy and secure multiparty computation. IEEE Transactions on Dependable and Secure Computing, 17(3), pp.530-543.

Zuboff, S. (2015) Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), pp.75-89.

APPENDIX 1 INTERVIEW TRANSCRIPTS

Transcript 1

	Question	Answer
Introduction		
	First of all, do you mind if I record this interview?	Yes, go ahead.
[Introduction to the study]		
[Statement that conveys the confidentiality and data usage aspects]		
	Can I use your name and the company that you are working for? Or else do you wish to provide a pseudonym or stay anonymous?	If you don't mind, I would like to stay anonymous.
	Can you please briefly describe your work experience in the Sri Lankan software development industry?	I've been in the software development industry for about six to seven years now. And I have worked for a couple of local companies mainly in the domain of ERP enterprise integrations.
	What is your current job role, and what are your responsibilities?	I'm the leader of the B2B communication product team. My main responsibilities are planning and execution of product enhancements for both SaaS platforms and our self-hostable software and I'm responsible for maintaining and managing release. I do attend requirement meetings and handle client support. I'm engaging in estimating and preparing budget plans for our self-hostable software and monitoring and controlling budget plans for cloud-based SaaS products as well. Other than that, I will be collecting progress reports from team members, and I report the status to the higher management.
	What is the nature of the software designed by your company?	Our company is a product-based company and as I mentioned earlier, we provide both self-hostable software and SaaS or cloud-based B2B software.
Privacy theme		
	As per your knowledge, How do you define 'Privacy'?	I think it's the expectation of a person protect self's assets or data from being accessed by unauthorized parties.
	Have you faced any difficulties when understanding privacy concepts and requirements?	Well, not right now. However, in the start of my career I had a lot of difficulties since I was not academically qualified. But some of my peers who had degrees, had a better understanding than me since they have learnt them in their universities.
	Are you involved in implementing privacy into the software developed by your company?	Yes, I'm involved in implementing privacy on different scales.
	What does your company do to ensure that the right privacy protection practices are in place?	We ensure that the users can only access data within their accounts, which is a part of the security aspect. When planning and designing the software deployments, we make sure to segregate client data storage as much as possible. For example, we use different cloud accounts for different client environments. When it comes to access controls and privileges, we are granting privileges to our internal team members to access our client systems and their data only for the purposes of analysis or troubleshooting. There we follow the principle of least privileges when granting access.

Sri Lankan data protection law theme		
	Are you familiar with the PERSONAL DATA PROTECTION ACT, No. 9 OF 2022? If yes, can you briefly explain.	I'm not much aware of the act, but I do remember reading a few articles on the topic of Personal Data Protection Act. From what I can recall, one of the intentions of the act is to protect the personal data of the Sri Lankan citizens. Considering the data collected by hospitals, banks, and other government entities. For example, during the recent COVID 19 pandemic situation, the health authorities collected personal data from citizens. I think based on all those facts the authorities have initiated and introduced this data protection act.
	Are you aware that there are certain Technical and Organizational Measures (TOM) that need to be considered when designing, developing, and implementing software to process personal data? If yes, can you comment on that?	Yes, I'm aware of, but I don't have that much knowledge about the specific measures to comment in a detailed manner.
	PERSONAL DATA PROTECTION ACT, No. 9 OF 2022 states that data encryption and pseudonymization as appropriate Technical and Organizational Measures (TOM), Do you have any work experience concerning these Technical and Organizational Measures (TOM)? If yes, can you briefly explain your experience with that?	Some of our clients have requested data encryption at rest, which we have provided using native features offered by cloud platform. Since AWS is our main cloud service provider, all Amazon S3 buckets have encryption configured by default, and all new objects uploaded to Amazon S3 are automatically encrypted by using server-side encryption with Amazon as keys. We have implemented those features into our software when we are providing our solutions to such customers who have requested and who are concerned and bound to comply with such privacy requirements.
Privacy by Design (PbD) theme		
	Are you familiar with the concept called 'Privacy by Design'? If yes, can you point out a few facts that you are familiar with?	Not entirely as a concept. In my opinion, privacy by design means designing the initial system structure itself to provide maximum possible privacy. Let's say for example, based on user data storage patterns or other factors, we have to secure those data by design itself in the initial state of the system structure designing stage rather than trying to segregate or isolate them later on through custom application or security rules.
	Are you aware of the seven foundational principles of Privacy by Design? If yes, can you comment on the seven foundational principles.	Yes, but I can't recall all seven principles at the moment. I'm aware that the privacy design should be user centric, and all the privacy policies should be transparent and communicated to the users appropriately. The systems by default should provide privacy and should take proactive measures rather than waiting for some issue to happen or occur.
	Privacy as the Default is one of the seven foundational principles of Privacy by Design and it means the maximum privacy protection should be provided to the users as a baseline. Can you recall any implementation done by your company that relates to this principle?	Sure, our software solutions are user centric, and all user data is stored in a private location which is accessible only by the specific user through a default dashboard login, and until he or she decides to expose it to any other systems by creating integrations or any entry points into set storage location. So, it's by default, only accessible to the particular user.
Embedding privacy theme		

	When you are developing a new software in your company, at which stage of the Software Development Life Cycle (SDLC) privacy is considered?	At the design stage mostly.
	Can you provide examples of specific practices or strategies your company follows to integrate privacy by design principles into the Software Development Life Cycle?	At the design stage, when we are preparing the design diagrams, we depict different services or platforms that the solution would ultimately use and draw the boundary of single user or organization across free services to understand which parts or stores may need to be shared, versus which can be actually totally segregated.
	Do you think there is a trade-off between implementing core functionality and embedding privacy in the design? What is your perception of this?	Yes, I think the design level privacy can compromise the performance of the solution. For example, by prohibiting the use of the shared infrastructure, which in turn affects the complexity and even the usability of the core functionalities of the software.
	In your work setup, who is held responsible for embedding privacy to the technology design of a software?	Speaking of our company, the relevant product owner and the technical leadership team of the company who are directly participating in the design phase, have the responsibility of embedding privacy into the software.
	What is the nature of the stakeholder collaboration when embedding privacy in to the Software Development Life Cycle?	Often privacy requirements or concerns are bought in by the customers themselves. We usually listen to their requirement over others because they are ultimately using the software.
	How does your company ensure that you and your team have the necessary knowledge and skills to implement privacy by design effectively?	Currently, there's no such official mechanism in place. Based on our own experiences we perform the work. Apart from that we don't have specific training or knowledge sharing mechanisms which cater privacy aspects.
	Assuming that you are given a chance to take an initiative for the integration of privacy into the software development lifecycle or to enhance the current practices, what would be your approach?	As the initial step, I would give the team an overview of the major privacy laws and regulations, since there is no such mechanism in our company, and I would review privacy practices published by the leading firms internationally and locally. Then I would review the designs and solution architectures of our current products and try to find out the weaknesses in the privacy implementations. I would take the required set of actions to rectify them and document them for future reference as well. And along with the team, I think I would prepare a set of privacy implementation guidelines for future products as well to mitigate the issues that we have already found in our existing customer deployments and solutions.
	Have you observed any specific examples or case studies where the integration of privacy by design has had a significant impact on the success or failure of a software development project? If so, would you like to share an example or a case study?	I don't think I have experienced any situation in that nature. But I can recall one of the famous incidents, there was an iCloud data privacy breach a couple of years ago, which had a significant impact on the stock values of Apple and iCloud market share. I believe the impact might have been much lesser if the proper privacy and data segregation mechanisms were in place and if they have considered privacy in the early stage of the project.
	"Embedding privacy into the technology design will allow the company to gain a competitive advantage" What is your perception on this statement?	Yes, rather than considering privacy as a legal or regulatory requirement, privacy can be considered as a must have function which will give the sense of safety and security. It's a strong selling point for any product that deals with user data. Actually, almost all the software out there in the market is involved with user data. So, the assurance of privacy can leverage competitive advantage.
Closure		

	Do you want to add anything relevant to the subject that we have not discussed during this interview?	Nothing specific to add. Thank you.
	[Thanking for the participation]	

Transcript 2

	Question	Answer
	Introduction	
	First of all, do you mind if I record this interview?	Okay, sure.
	[Introduction to the study]	
	[Statement that conveys the confidentiality and data usage aspects]	
	Can I use your name and the company that you are working for? Or else do you wish to provide a pseudonym or stay anonymous?	I would like to stay anonymous.
	Can you please briefly describe your work experience in the Sri Lankan software development industry?	I've been working as a Senior Information Security Analyst at a leading cybersecurity firm in Sri Lanka for nearly six years. My role as a security analyst is to conduct security compliance reviews based on various local and robust security standards. Such as PCI DSS standard, ISO 7001, ISO 2002 and, NIST security standards.
	What is your current job role, and what are your responsibilities?	I'm currently working as a Senior Information Security Analyst at a leading cybersecurity firm in Sri Lanka and also as a visiting lecturer for cybersecurity law at a private university.
	What is the nature of the software designed by your company?	As a company we provide security consultations, basically for the clients from the banking sector, telco and for software development companies. Basically, when it comes to consultation, we're doing security assessments like vulnerability assessments, penetration testing, information security and operational assessments, antivirus assessments, also security code reviews.
	Privacy theme	
	As per your knowledge, How do you define 'Privacy'?	In my opinion, privacy is one's right to safeguard and control their personal information. Data protection measures are used to protect personal data by ensuring confidentiality and privacy. So, when it comes to privacy, there are various areas to pay attention to. One such area is personal data protection. With the GDPR, personal data protection has been highlighted in the last few years. Individuals have the right to know how their personal information is being used, the right to know who is collecting the data, and for what purpose. Privacy is one of the rights of the bodily autonomy to take actions and make decisions. Like you can have the right to express yourself about specific topics when it comes to politics or sexual orientation or religion. So, I think it's a right of an individual. I think privacy is a right. A country should maintain it as a right, and it's one's right to control their personal information.

	Have you faced any difficulties when understanding privacy concepts and requirements?	Actually, it was somewhat difficult like two to three years ago. But with the impact of the GDPR, privacy became a huge topic. With that I researched different areas in privacy and the concepts associated with privacy. As a result of the continuous learning now I have familiarized myself with privacy terms and concepts. Therefore, I can understand privacy related requirements better compared to earlier.
	Are you involved in implementing privacy into the software developed by your company?	As a firm we provide consultations and guidance with regard to privacy implementations and compliances. I engage in reviewing compliance standards based on various global security standards. For example, PCI DSS is a security standard that the banking sector used to ensure the security of credit card information. So, the credit card information is someone's personal data, right? Your bank account details, and your PIN number are your personal data. When it comes to the clients from the banking sector, the main question from the clients is how we can protect the customer's personal data? As a consultation company, we are advising them to collect the minimum amount of personal that is required for the purpose. We do highlight about taking data backups in a secure way. Not only that, the use of proper security mechanisms when storing data also important. Likewise, those are some of the ways that I have involved in providing consultations for implementing privacy in the local software development industry.
	What does your company do to ensure that the right privacy protection practices are in place?	I would say the basic security measures are implemented in our company. For example, it is mandatory for us to maintain backups of our work and we are only allowed to use the laptop and other equipment provided by the office for the work-related tasks and no personal devices are allowed to store any work-related data Since we are dealing with client's data, so we have to ensure the security and the confidentiality of data. Also, the access control mechanisms are in place.
Sri Lankan data protection law theme		
	Are you familiar with the PERSONAL DATA PROTECTION ACT, No. 9 OF 2022? If yes, can you briefly explain.	Yes, I'm familiar with the Personal Data Protection Act which was passed by the Parliament recently. Personal Data Protection Act provides the regulations, or the laws related to the processing of personal data. With the Act, the trust in software systems that processes personal data will be improved, online transactions or online activities are going to be securely processed and the personal data will be securely processed.
	Are you aware that there are certain Technical and Organizational Measures (TOM) that need to be considered when designing, developing, and implementing software to process personal data? If yes, can you comment on that?	Yes, I do. But I can't recall the exact section now. Simply the PDPA wants to make sure that the technical and organizational measures are in place when processing personal data. For example, let's say a software development company which is developing new software, can use data encryption. Also, the access control mechanisms and authentication methods like two-factor authentication. They can even use pseudonyms to safeguard the identify the individuals.

	PERSONAL DATA PROTECTION ACT, No. 9 OF 2022 states that data encryption and pseudonymization as appropriate Technical and Organizational Measures (TOM), Do you have any work experience concerning these Technical and Organizational Measures (TOM)? If yes, can you briefly explain your experience with that?	Yes, like I said earlier we often advise our clients on the importance of data encryption, especially when it comes to our banking sector clients. As a company, we also follow mechanisms like encryption when storing our client's data.
	Privacy by Design (PbD) theme	
	Are you familiar with the concept called 'Privacy by Design'? If yes, can you point out a few facts that you are familiar with?	Yes, I have come across this concept. Simply how data can be protected from the technology design itself.
	Are you aware of the seven foundational principles of Privacy by Design? If yes, can you comment on the seven foundational principles.	Actually, in the framework there are seven principles that needed to be considered when implementing privacy from the design perspective. But the reality all seven principles are not being considered. But the principle of privacy by default is commonly used and practiced.
	Privacy as the Default is one of the seven foundational principles of Privacy by Design and it means the maximum privacy protection should be provided to the users as a baseline. Can you recall any implementation done by your company that relates to this principle?	Like I said earlier, privacy by default is widely known but unfortunately most of the clients don't consider this early. Actually, after the completion of the software development, then only privacy is becoming a major concern and by that time it's very difficult to change the functionality and the design. Even that's the case, most of the clients use secure coding guidelines. As per those guidelines there are specific requirements that the developers must maintain when developing the software. So eventually the principle of privacy by default is addressed here.
	Embedding privacy theme	
	When you are developing a new software in your company, at which stage of the Software Development Life Cycle (SDLC) privacy is considered?	Yeah, I think in almost all the stages privacy must be considered. Frankly speaking, in the requirement gathering stage privacy requirements needed to be clearly discussed and set the expectations accordingly. Then only the rest of the stages can follow the necessary steps.
	Can you provide examples of specific practices or strategies your company follows to integrate privacy by design principles into the Software Development Life Cycle?	There are some situations where the client is unable to follow all the privacy related requirements, in such a situation we are suggesting them compensating controls or requirements depending on the compliances and the context. For example, the actual requirement is to have daily backups but if it's not possible due to any proper reason then as compensation control, we can suggest to keep weekly backups. Likewise, that's one of the strategies suggested by us.
	Do you think there is a trade-off between implementing core functionality and embedding privacy	Yes, my personal view is that privacy requirements should not be compromised.

	in the design? What is your perception of this?	When providing consultations, I have seen that clients often consider security requirements after completing the development of the software where the privacy related requirements are disregarded at the initial stages. Even if the client wants to embed privacy features by that time, it will be a complicated process since the design and development stages are already completed.
	In your work setup, who is held responsible for embedding privacy to the technology design of a software?	Responsibility-wise, I can't pinpoint one role and say that this role is primarily responsible for embedding privacy into the project. In my opinion, the entire team setup has the responsibility but some of the roles have extra responsibilities compared to others. For example, team leads and Chief Information Security Officer as well. In short, it is a shared responsibility.
	What is the nature of the stakeholder collaboration when embedding privacy in to the Software Development Life Cycle?	The stakeholders play an important role so they should be aware of the importance of privacy. If you look at the European Union region, the clients are keen on privacy. Likewise, we need to encourage the same in Sri Lanka. With the Personal Data Protection Act, I believe that there will be a considerable improvement in terms of awareness. As a software development company, following privacy practices and secure coding guidelines won't be sufficient. The companies should initiate discussions with their clients to enhance the privacy of the software that they build. With that productive interaction or collaboration will happen.
	How does your company ensure that you and your team have the necessary knowledge and skills to implement privacy by design effectively?	The Security Engineers and the Consultants are specialized in Information Security discipline. To keep ourselves up to date with the emerging technologies, security practices and legal aspects, we have a weekly meeting like a knowledge sharing session where one person from the team will pick a topic and do a presentation to the entire team on the selected topic or the area. The intention of this session is to encourage continuous learning.
	Assuming that you are given a chance to take an initiative for the integration of privacy into the software development lifecycle or to enhance the current practices, what would be your approach?	My first piece of advice is to start early. When planning and designing the software, privacy requirements needed to be considered. The software must minimize the collection of personal data. The developers have to follow industry best practices and secure coding guidelines. The required policies have to be implemented with regard to retaining the collected personal data, once the purpose is fulfilled those data needed to be discarded. Additionally, the security mechanisms like data encryption, secure data sharing and data backups needed to be implemented. If the client can pay attention to these basic requirements as early as possible then the privacy can be preserved in the software.
	Have you observed any specific examples or case studies where the integration of privacy by design has had a significant impact on the success or failure of a software development project? If so, would you like to share an example or a case study?	I can't name a specific client, but I have seen incidents which caused negative impacts to clients due to poor security requirement implementation. We can study such use cases to mitigate such security risks in upcoming projects.
	"Embedding privacy into the technology design will allow the company to gain a	Absolutely. I'm working closely with banking clients in Sri Lanka. As a result of that, I'm familiar with many mobile banking applications currently operating in the market.

	competitive advantage" What is your perception on this statement?	I have noticed some banking clients who are a bit reluctant to consider privacy as a vital requirement whereas some clients are treating privacy factors in a peculiar way. Because they know it will help them to gain the trust of their customers. The end users, I mean the banking customers, they are coming from different demographic segments. The tech-savvy customers are usually aware of an online transaction process, but some customers may get reluctant to do an online transaction right away. To win customers coming from different backgrounds, the software applications needed to be designed and developed in a simple yet secure manner. If the right privacy principles are embedded to the software, then that will definitely add a value which will lead to competitive advantage.
Closure		
	Do you want to add anything relevant to the subject that we have not discussed during this interview?	I guess we covered many areas so nothing more to add specifically. Thank you.
[Thanking for the participation]		

Transcript 3

	Question	**Answer**
Introduction		
	First of all, do you mind if I record this interview?	Yes, No Problem.
[Introduction to the study]		
[Statement that conveys the confidentiality and data usage aspects]		
	Can I use your name and the company that you are working for? Or else do you wish to provide a pseudonym or stay anonymous?	Let's go with Hashan & I closely work with telecommunications industry.
	Can you please briefly describe your work experience in the Sri Lankan software development industry?	I've been in the software development industry in Sri Lanka for over five years. My work has mainly involved developing and enhancing product features for customer and retailer support applications within the telecommunications sector.
	What is your current job role, and what are your responsibilities?	I'm a DevOps Engineer working on features for customer and retailer support applications of the Telco corporation we were employed with. I'm deeply involved in deployment having to do with seamless integration of new features and system stability. I work hand in hand with the development team to automate our CI/CD pipeline, and manage infrastructure for an array of applications. I also manage system monitoring and troubleshooting, so that we quickly address any problems in order to provide the best service for our users.
	What is the nature of the software designed by your company?	Our company is focused on developing software for the telecommunications industry, specifically customer and retailer support applications. We design solutions that enhance user experience by improving the functionality and features of these applications.

Privacy theme		
	As per your knowledge, How do you define 'Privacy'?	I believe privacy is about safeguarding personal data and information from being accessed or misused by unauthorized individuals or entities. Also privacy should also respect the legal requirements which comes from both through privacy agreements and the general law.
	Have you faced any difficulties when understanding privacy concepts and requirements?	Difficulties are part and partial of this job. But with experience I have lesser difficulties, since I now I know what to do in most of the challenges. Just like in other fields, anyone can do better in estalbslihing privacy when they involve in more and more software development projects.
	Are you involved in implementing privacy into the software developed by your company?	Yes. I'm involved in.
	What does your company do to ensure that the right privacy protection practices are in place?	We take privacy very seriously and limit access to data through our customer or retailer support applications as much as possible. Users can only see the minimum data needed to fulfill their job, reducing risk of unauthorized access to information. We implement additional data storage isolation for each client, especially useful within the telecommunications sector where sensitive customer information is commonly managed. That means, you may be dealing with not using the same cloud for all customers so that data of customer A is kept separated from Customer B & so on. Additionally, we follow stringent access control protocols, granting our internal team members access to client data strictly on a need-to-know basis, such as for troubleshooting or support purposes. By adhering to the principle of least privilege, we further minimize the potential for data exposure, ensuring that privacy is deeply integrated into our software design and operations.
Sri Lankan data protection law theme		
	Are you familiar with the PERSONAL DATA PROTECTION ACT, No. 9 OF 2022? If yes, can you briefly explain.	I'm somewhat familiar with the Personal Data Protection Act, No. 9 of 2022 since I'm more close to the customer information. From what I've read, the act is designed to safeguard the personal data of Sri Lankan citizens. The act emphasizes the importance of protecting data collected from customers, ensuring that their privacy is maintained throughout the data lifecycle. For example, in the telecom industry, where we manage a significant amount of customer data through support applications, this act would require us to implement strict data protection measures, such as minimizing data collection and securing any data that is stored or processed. The goal is to ensure that customer information is handled responsibly and securely, in line with the legal requirements.
	Are you aware that there are certain Technical and Organizational Measures (TOM) that need to be considered when designing, developing, and implementing software to process personal data? If yes, can you comment on that?	Yes, I am aware of them for the most extent.
	PERSONAL DATA PROTECTION ACT, No. 9 OF 2022 states that data encryption and pseudonymization as appropriate Technical and Organizational Measures (TOM), Do you have any work experience concerning these	Yes, I have experience with data encryption and pseudonymization as Technical and Organizational Measures. For instance, we use encryption to secure customer data, which is crucial in the telecom industry. In our projects, we implement data encryption both at rest and in transit. For data at rest, we use encryption tools provided by our cloud services to ensure that all stored data is protected. For data in transit, we use TLS/SSL protocols to secure the data as it moves between systems. This approach helps us meet privacy

	Technical and Organizational Measures (TOM)? If yes, can you briefly explain your experience with that?	requirements and ensures that sensitive customer information is safeguarded throughout its lifecycle.
	Privacy by Design (PbD) theme	
	Are you familiar with the concept called 'Privacy by Design'? If yes, can you point out a few facts that you are familiar with?	I'm somewhat familiar with the concept of 'Privacy by Design.' To me, it means integrating privacy measures right from the start when designing the system. For example, in our telecom applications, this could involve planning for data encryption and secure data storage right from the design phase rather than adding these features later. This approach ensures that privacy is built into the system's architecture, rather than being an afterthought, which helps us better protect customer data from the outset.
	Are you aware of the seven foundational principles of Privacy by Design? If yes, can you comment on the seven foundational principles.	Yes, I'm familiar with the seven foundational principles of Privacy by Design, though I don't recall all of them off the top of my head. I do know that the principles emphasize a user-centric approach, ensuring that privacy is at the core of system design. This means privacy policies should be clear and communicated effectively to users. Additionally, privacy should be built into the system by default, and we should take proactive steps to safeguard data rather than waiting for issues to arise.
	Privacy as the Default is one of the seven foundational principles of Privacy by Design and it means the maximum privacy protection should be provided to the users as a baseline. Can you recall any implementation done by your company that relates to this principle?	Certainly. In our telecom applications, we ensure privacy as the default by making sure that customer data is stored in secure, isolated environments. By default, only the specific user has access to their own data through a secure login. This setup means that unless a user actively chooses to share their data through integrations or external systems, their information remains private and inaccessible to others. This approach helps us adhere to the principle of providing maximum privacy protection right from the start.
	Embedding privacy theme	
	When you are developing a new software in your company, at which stage of the Software Development Life Cycle (SDLC) privacy is considered?	Obviously at the design stage.
	Can you provide examples of specific practices or strategies your company follows to integrate privacy by design principles into the Software Development Life Cycle?	At the planning phase, we map out the entire customer journey within our telecom applications. For instance, we identify which customer data needs to be isolated within specific modules, like billing or support, and ensure that access controls are set up accordingly. We also design systems with built-in encryption and access logging for sensitive data, so that privacy considerations are addressed right from the start. This approach helps us maintain a high level of data protection and ensures that privacy is integral to our software's architecture.
	Do you think there is a trade-off between implementing core functionality and embedding privacy in the design? What is your perception of this?	Yes, there can be a trade-off between embedding privacy and core functionality. For instance, adding strong encryption and strict access controls can sometimes slow down system performance or add complexity to the user experience. In applications we design, this might mean slower data processing times or a more cumbersome user interface when privacy measures are fully integrated. Balancing these aspects is crucial to ensure that privacy enhancements do not unduly impact the core functionalities or user satisfaction.

	In your work setup, who is held responsible for embedding privacy to the technology design of a software?	In our setup, the responsibility for embedding privacy into technology design falls primarily on the product managers and the security team. They work closely during the design phase to ensure that privacy considerations are integrated from the start. Additionally, our compliance officers review the designs to ensure they meet all relevant privacy regulations and standards.
	What is the nature of the stakeholder collaboration when embedding privacy in to the Software Development Life Cycle?	Primarily, requirements are brought in by the product managers based on industry standards & customers' concerns.
	How does your company ensure that you and your team have the necessary knowledge and skills to implement privacy by design effectively?	Our company ensures that the team is well-equipped to implement privacy by design by providing specific training on data protection and privacy principles. We have regular sessions and workshops to keep everyone updated on the latest privacy regulations and best practices. Additionally, during the hiring process, we assess candidates' understanding of privacy by design to ensure they meet our standards.
	Assuming that you are given a chance to take an initiative for the integration of privacy into the software development lifecycle or to enhance the current practices, what would be your approach?	I'd start by conducting a comprehensive review of current privacy laws in the general context and also relevant to the telecom industry. I'd then assess our existing software architectures and identify any gaps in privacy protection. Next, I'd implement improved privacy measures and develop updated guidelines based on both local and global best practices. I'd also set up regular training sessions to ensure the team is always informed about the latest privacy standards and practices.
	Have you observed any specific examples or case studies where the integration of privacy by design has had a significant impact on the success or failure of a software development project? If so, would you like to share an example or a case study?	I haven't encountered a specific case, however, a well-known example is the Facebook-Cambridge Analytica scandal. The breach exposed how user data was improperly accessed and used, which severely damaged Facebook's reputation and led to substantial regulatory scrutiny and fines. This incident highlighted the critical importance of integrating privacy by design from the outset to avoid such risks and to protect user data effectively. These incidents gives bad image ot both the developers and the client firm.
	"Embedding privacy into the technology design will allow the company to gain a competitive advantage" What is your perception on this statement?	Yes, I believe embedding privacy into technology design can indeed offer a competitive advantage. For example, if our applications for customer and retailer support feature advanced privacy controls by default, it builds trust with users. This can be a significant selling point, especially when dealing with sensitive customer data like call records or personal details. Essentially, demonstrating strong privacy practices can enhance customer confidence and differentiate our services in a crowded market.
Closure		
	Do you want to add anything relevant to the subject that we have not discussed during this interview?	It seems we've covered all the key areas, so, Thank you!
[Thanking for the participation]		

Transcript 4

	Question	**Answer**
Introduction		

	First of all, do you mind if I record this interview?	Okay
[Introduction to the study]		
[Statement that conveys the confidentiality and data usage aspects]		
	Can I use your name and the company that you are working for? Or else do you wish to provide a pseudonym or stay anonymous?	I like to stay anonymous. And, my company is branch of a global business which involves in designing and managing loyalty programs across the globe, leveraging data to make brands smarter.
	Can you please briefly describe your work experience in the Sri Lankan software development industry?	I have over 10 years of experience in the commercial software development sector in Sri Lanka, primarily focusing on building and improving customer-centric applications using modern frameworks like React, with expertise in cloud-based architectures.
	What is your current job role, and what are your responsibilities?	I work as a Senior Software Engineer, responsible for developing and maintaining program code according to system designs, enhancing application functionality, and ensuring code quality through testing and debugging. I also collaborate closely with tech leads and senior engineers in sprint planning, and I'm involved in CI/CD pipeline management, version control, and documentation.
	What is the nature of the software designed by your company?	Our software enables brands to create personalized, engaging consumer experiences at scale, primarily through AI-driven loyalty and CRM platforms that enhance customer relationships and lifetime value.
Privacy theme		
	As per your knowledge, How do you define 'Privacy'?	To my understanding, privacy is safeguarding personal data from unauthorized access, ensuring control over information sharing and usage.
	Have you faced any difficulties when understanding privacy concepts and requirements?	No, with over 10 years of experience, I have a solid grasp of privacy concepts and requirements. But this was not the case when I started working. Back then I had many confusions, mistakes and stress on how to meet the privacy requirement of a project. No matter what books you have read on privacy, things are different when you are in practical environment. Litte by little with more experience, I do not have difficulties, since I know things in and out.
	Are you involved in implementing privacy into the software developed by your company?	Yes, I actively integrate privacy measures into our software design.
	What does your company do to ensure that the right privacy protection practices are in place?	At our company, we make privacy a top priority by applying Privacy by Design principles throughout the entire software development process. We hold regular training sessions to keep our team informed about the latest privacy laws and best practices. During the design phase, we work closely with our legal and compliance teams to make sure all privacy requirements are met. We also carry out detailed privacy impact assessments and continuously check and audit our systems to ensure they stay compliant. Our AI-native platform is built with data protection as a fundamental feature, allowing brands to handle customer data safely and responsibly, which helps build trust and boost customer loyalty.
Sri Lankan data protection law theme		

	Are you familiar with the PERSONAL DATA PROTECTION ACT, No. 9 OF 2022? If yes, can you briefly explain.	Yes, I'm familiar with the act. It sets clear guidelines for protecting personal data in Sri Lanka, making sure organizations manage data responsibly and securely. It requires companies to use security measures like data encryption and pseudonymization to protect against unauthorized access and data breaches. The act also outlines individuals' rights to access, correct, and delete their data, and it mandates that companies appoint data protection officers to ensure they follow these rules.
	Are you aware that there are certain Technical and Organizational Measures (TOM) that need to be considered when designing, developing, and implementing software to process personal data? If yes, can you comment on that?	Yes, these measures include using data encryption, setting up access controls, and conducting regular security audits to protect personal data at every stage of the software development process.
	PERSONAL DATA PROTECTION ACT, No. 9 OF 2022 states that data encryption and pseudonymization as appropriate Technical and Organizational Measures (TOM), Do you have any work experience concerning these Technical and Organizational Measures (TOM)? If yes, can you briefly explain your experience with that?	Yes, I've worked with data encryption and pseudonymization in software projects. Recently, we used AES-256 encryption to protect sensitive customer data both when it was stored and while being transferred. We also used pseudonymization to keep customer data anonymous during development and testing, making sure we didn't expose real data unnecessarily. These steps were crucial for meeting both legal standards and our clients' security needs.
Privacy by Design (PbD) theme		
	Are you familiar with the concept called 'Privacy by Design'? If yes, can you point out a few facts that you are familiar with?	Yes, I'm familiar with Privacy by Design. It's about making privacy a key part of IT system design from the very beginning. This means that privacy isn't just added on later but is built into the system right from the start. It involves practices like data minimization, where we only collect the data we really need, and user consent, giving users control over their own data. Essentially, Privacy by Design focuses on preventing privacy issues before they arise, taking a proactive approach to protecting data.
	Are you aware of the seven foundational principles of Privacy by Design? If yes, can you comment on the seven foundational principles.	Yes, I'm aware of the seven key principles of Privacy by Design. They focus on being proactive about privacy, making it the default setting, and building it into the system from the start. These principles also stress the importance of ensuring full functionality, keeping security intact throughout, being transparent, and respecting user privacy throughout the system's life. Essentially, these principles make sure privacy is a fundamental part of the system, rather than something added on later.
	Privacy as the Default is one of the seven foundational principles of Privacy by Design and it means the maximum privacy protection should be provided to the users as a baseline. Can you recall any implementation done by your company that relates to this principle?	Yes, our company usually sets all user data settings to the highest privacy level by default. This means that unless users actively change their settings, their data stays private and isn't collected or shared unnecessarily. For example, our user accounts are set to require clear consent before collecting any data, giving users control over what information is shared. This way, we follow the "Privacy as the Default" principle and make sure user data is protected right from the start.
Embedding privacy theme		
	When you are developing a new software in your company, at which stage of the Software	Privacy is considered from the very beginning, during the planning and design phases of the SDLC.

	Development Life Cycle (SDLC) privacy is considered?	
	Can you provide examples of specific practices or strategies your company follows to integrate privacy by design principles into the Software Development Life Cycle?	We integrate privacy by design through multiple strategies. First, we conduct privacy impact assessments during the planning phase to identify potential risks. During development, we ensure that data minimization is practiced, collecting only what is necessary. Encryption and anonymization techniques are applied to protect sensitive data. We also incorporate user consent mechanisms, ensuring that users have control over their data. Finally, we conduct regular audits and code reviews to ensure that privacy standards are maintained throughout the SDLC.
	Do you think there is a trade-off between implementing core functionality and embedding privacy in the design? What is your perception of this?	While there can be a perceived trade-off, I believe privacy and functionality should coexist. Embedding privacy doesn't mean sacrificing core features; rather, it's about thoughtful design. By integrating privacy from the start, we can create systems that are both functional and secure. It may require more effort initially, but it builds trust with users and ensures compliance with regulations, which ultimately benefits the business in the long run.
	In your work setup, who is held responsible for embedding privacy to the technology design of a software?	Responsibility for embedding privacy is shared among the development team, particularly the lead engineers, along with input from the legal and compliance departments.
	What is the nature of the stakeholder collaboration when embedding privacy in to the Software Development Life Cycle?	Collaboration is cross-functional, involving developers, product managers, legal teams, and security experts. Regular meetings ensure that privacy concerns are addressed at each stage of the development process.
	How does your company ensure that you and your team have the necessary knowledge and skills to implement privacy by design effectively?	Our company places a strong emphasis on continuous learning. We regularly attend workshops and training sessions focused on privacy laws, data protection, and secure coding practices. We also have access to online courses and certifications related to privacy by design. Additionally, we participate in internal knowledge-sharing sessions where team members discuss recent privacy challenges and solutions. This approach ensures that everyone stays updated on the best practices and emerging trends in privacy by design.
	Assuming that you are given a chance to take an initiative for the integration of privacy into the software development lifecycle or to enhance the current practices, what would be your approach?	If given the chance, my approach would start with conducting a comprehensive privacy risk assessment at the very beginning of the project. I would advocate for incorporating privacy requirements into the initial design specifications and establish a clear process for continuous monitoring and auditing throughout the development lifecycle. Additionally, I would introduce regular privacy training sessions for the team and ensure that we implement user feedback loops to improve privacy features based on real-world usage.
	Have you observed any specific examples or case studies where the integration of privacy by design has had a significant impact on the success or failure of a software development project? If so, would you like to share an example or a case study?	As you know Privacy related incident comes by surprise. So I cannot clearly say tha we made this particualr privacy improvement, so it prevented a particular incident. But if we get to know that a particular incident occurred in a product developed by some other company. We can assess our privacy mechanisms and check whether it could happen to us as well. If we find out that our privacy mechanisms are strong and such an incident would not happen, now that is a point where we know how our mechanisms have prevented a bad privacy incident.
	"Embedding privacy into the technology design will allow the company to gain a competitive advantage" What is your perception on this statement?	I strongly agree with this statement. In today's market, users are increasingly concerned about their data privacy. Companies that prioritize privacy not only comply with regulations but also build trust with their customers. This trust can differentiate a company from its competitors, leading to increased customer loyalty, and ultimately, a competitive advantage in the market.
Closure		

	Do you want to add anything relevant to the subject that we have not discussed during this interview?	I would like to emphasize that privacy by design is not just a technical challenge but also a cultural one. Building a culture that values and prioritizes privacy at every level of the organization is crucial. This cultural shift will ensure that privacy considerations are embedded naturally into every project, leading to more secure and trustworthy products.
	[Thanking for the participation]	

Transcript 5

	Question	**Answer**
	Introduction	
	First of all, do you mind if I record this interview?	Sure.
	[Introduction to the study]	
	[Statement that conveys the confidentiality and data usage aspects]	
	Can I use your name and the company that you are working for? Or else do you wish to provide a pseudonym or stay anonymous?	Well, I would prefer to be anonymous. But I can tell you about my industry without any names. Currently the company I work for is one of top 5 IT sector companies in Sri Lanka
	Can you please briefly describe your work experience in the Sri Lankan software development industry?	But I can tell you about my industry without any names. I have been working an business analyst for nearly 5 years, for two IT firms in Sri Lanka. In my experience I have handled software developments for various local conglomerates and foreign enterprises.
	What is your current job role, and what are your responsibilities?	In my role as a senior software engineer, my responsibilities include creating and managing program code in accordance with system designs, improving the functionality of applications, and guaranteeing code quality through debugging and testing. In addition, I work closely with senior engineers and tech leads to plan sprints. I also handle version control, documentation, and the CI/CD pipeline.
	What is the nature of the software designed by your company?	The company I have work for in the past and my current employer has a large scope of software designed. But the projects which I have mostly involved are into integrated solutions and CRM
	Privacy theme	
	As per your knowledge, How do you define 'Privacy'?	What I see as Privacy is making sure someone's personal or sensitive information being non-accessible to anyone who is not being authorized.
	Have you faced any difficulties when understanding privacy concepts and requirements?	Well so far there are no such cases. But privacy is an evolving concept, so you must keep understand it in new ways. There could be new challenges in future.
	Are you involved in implementing privacy into the software developed by your company?	Yes, I have direct involvement with setting up the privacy policies and certain other conditions to ensure privacy.

	What does your company do to ensure that the right privacy protection practices are in place?	By implementing Privacy by Design principles throughout the software development process, our organization places a high priority on privacy. There are frequent training sessions, teamwork with legal and compliance departments, and thorough privacy effect analyses. We enforce strict access control procedures, build extra data storage separation, and restrict access to data through customer or retailer support applications. Especially for the employee we allow access through separate accounts to ensure they do not have access beyond their level. on the other hand, we agree with the client on who and who will be getting access to which kind of data. By reducing data exposure even further, the principle of least privilege guarantees that privacy is thoroughly ingrained in our software's development and functioning.
Sri Lankan data protection law theme		
	Are you familiar with the PERSONAL DATA PROTECTION ACT, No. 9 OF 2022? If yes, can you briefly explain.	I have a basic understanding of the Personal Data Protection Act, No. 9 of 2022, as I work closely with client data. The measure is intended to protect Sri Lankan nationals' personal information, based on what I've read. The act places a strong emphasis on safeguarding consumer data and making sure that their privacy is upheld throughout the data lifecycle. For instance, this act will compel us to put in place stringent data protection measures, like limiting data collecting and safeguarding any data that is processed or stored, in the telecom sector, where we handle a substantial quantity of customer data through support applications. Ensuring that customer information is handled safely, ethically, and in compliance with the law is the aim.
	Are you aware that there are certain Technical and Organizational Measures (TOM) that need to be considered when designing, developing, and implementing software to process personal data? If yes, can you comment on that?	Well, I am not the best to comment on this, but to my knowledge things like data protection measures from unauthorized access, measures of encrypting, defined practices for coding are important. I believe audits also play a key role.
	PERSONAL DATA PROTECTION ACT, No. 9 OF 2022 states that data encryption and pseudonymization as appropriate Technical and Organizational Measures (TOM), Do you have any work experience concerning these Technical and Organizational Measures (TOM)? If yes, can you briefly explain your experience with that?	In terms of organizational and technical measures, I have experience with data encryption and pseudonymization. One important use in the telecom sector is encryption, which we utilize to safeguard client data. We utilize both in-transit and at-rest data encryption in our projects. We utilize encryption technologies offered by our cloud services to guarantee the security of all data that is stored in the background. To protect data when it is being transferred between computers, we employ TLS/SSL protocols. Our strategy guarantees that sensitive customer data is protected at every stage of its lifetime and assists us in meeting privacy regulations.
Privacy by Design (PbD) theme		
	Are you familiar with the concept called 'Privacy by Design'? If yes, can you point out a few facts that you are familiar with?	Yeah, I am familiar with that. The main idea behind that is the enforcement of privacy into the designs so any privacy matters can be proactively minimized. So, the main argument here is to be proactive not reactive. This includes design being transparent on the data use and paying attention to all matters that impacts privacy.
	Are you aware of the seven foundational principles of Privacy by Design? If yes, can you comment on the seven foundational principles.	Of course, yes. Well, the first one is as I said to be proactive rather than reactive to privacy matters. Second is the privacy is safeguarded in all parts mandatorily, without considering it as a special case. Third is the identification of privacy as a core functional element of the system. 4th is that any request or objective that is critical to privacy should be met. Next is the end-to-end security where data is protected throughout the cycle. Next is that

		it should be transparent on how the data is used. This I said before as well. Final one having respect for privacy.
	Privacy as the Default is one of the seven foundational principles of Privacy by Design and it means the maximum privacy protection should be provided to the users as a baseline. Can you recall any implementation done by your company that relates to this principle?	Yes, I can draw examples from many of my past CRM projects. For example, one big privacy by design elements is the limited data collection or not collecting data pieces that not required. This is key at a basic level to ensure privacy. If CRM does not want the customer photo, you do not want to get it. Another one is the case-by-case review of data access to each team. This prevents certain employees from accessing unauthorized data by loopholes in classification.
Embedding privacy theme		
	When you are developing a new software in your company, at which stage of the Software Development Life Cycle (SDLC) privacy is considered?	Well, most certainly from the very beginning of the cycle.
	Can you provide examples of specific practices or strategies your company follows to integrate privacy by design principles into the Software Development Life Cycle?	We design the whole client journey within our telecom applications throughout the planning stage. For example, we determine whether client information must be kept separate within modules, such as support or billing, and make sure that access restrictions are configured appropriately. Additionally, we incorporate access logging and encryption into our systems' design for sensitive data, ensuring that privacy concerns are taken care of from the outset. This strategy guarantees that privacy is ingrained in the design of our products and helps us maintain a high standard of data security.
	Do you think there is a trade-off between implementing core functionality and embedding privacy in the design? What is your perception of this?	Certainly, there may be a trade-off between privacy integration and essential features. Strong encryption and stringent access controls, for example, may occasionally cause system performance to lag or increase user experience complexity. When privacy controls are completely integrated, this may result in slower data processing times or a more complicated user interface in the applications we build. To guarantee that privacy improvements do not unnecessarily affect essential features or user pleasure, it is imperative to strike a balance between these factors.
	In your work setup, who is held responsible for embedding privacy to the technology design of a software?	Privacy is a collective responsibility. But the extent of responsibility differs in different stages. When making a framework for privacy, the legal teams bear responsibilities. But imagine if a specified privacy element is not in the final delivery, then the development team is more responsible.
	What is the nature of the stakeholder collaboration when embedding privacy in to the Software Development Life Cycle?	Well mostly the collaboration with stakeholders happens through meetings. These meetings will involve development teams, legal teams and product teams to come to a conclusion on the privacy matters. Then the subsequent meetings will review the progress of the agreed privacy measures.
	How does your company ensure that you and your team have the necessary knowledge and skills to implement privacy by design effectively?	In our organization, we do have weekly knowledge-sharing sessions in which we focus on different topics related to software development trends and security topics. During those sessions, we usually share our own previous implementation experiences as well.

	Assuming that you are given a chance to take an initiative for the integration of privacy into the software development lifecycle or to enhance the current practices, what would be your approach?	I recommend developing a continuous monitoring and auditing procedure throughout the development lifecycle, including privacy requirements into design specifications, and doing a thorough privacy risk assessment.
	Have you observed any specific examples or case studies where the integration of privacy by design has had a significant impact on the success or failure of a software development project? If so, would you like to share an example or a case study?	Well, thoughout my career I have seen how we have learned from the privacy related negative incidents in the past and then implement better measures in future projects. As a result we have saved a lot of clients from experiencing privacy related negative incidents. This improvements have created a lot of trust about us as a developer in the client minds. Also our good efforts allows us to position as a more secure solutions provider.
	"Embedding privacy into the technology design will allow the company to gain a competitive advantage" What is your perception on this statement?	Incorporating privacy into technology design can, in my opinion, provide a competitive edge. Users would feel more trusted, for instance, if our applications for store and customer support come with sophisticated privacy protections by default. This can be a powerful selling factor, particularly when handling sensitive data. In essence, exhibiting sound privacy procedures can boost client confidence and set our services apart in a congested market.
Closure		
	Do you want to add anything relevant to the subject that we have not discussed during this interview?	Let me say this as a closing note, when a corporate culture has more respect for privacy, you have less potential for privacy breaches. So I appreciate getting the chance to express my ideas on this topic.
[Thanking for the participation]		

Transcript 6

	Question	**Answer**
Introduction		
	First of all, do you mind if I record this interview?	Okay, sure.
[Introduction to the study]		
[Statement that conveys the confidentiality and data usage aspects]		
	Can I use your name and the company that you are working for? Or else do you wish to provide a pseudonym or stay anonymous?	I ‘m Dhanika Perera, a change-making Serial Entrepreneur and the Chief Executive Officer of Bhasha Lanka (Pvt) Ltd.
	Can you please briefly describe your work experience in the Sri Lankan software development industry?	First of all, I am a founder of several pioneering software products that are specifically targeting the Sri Lankan market. Namely we have key software products out in the Sri Lankan market as “Helakuru”, “PayHere” and “Hapan” which are targeting multiple market segments in the country.
	What is your current job role, and what are your responsibilities?	Apart from my entrepreneurial and managerial tasks, I have been involved in founding the products “Helakuru”, “PayHere” and “Hapan”. On top of that I am contributing as the Product Designer and User Experience Designer for all these products.

	What is the nature of the software designed by your company?	Our “Helakuru” product is a mass market product which provides consumer software services, software as a service for the consumers in Sri Lanka. And “PayHere” is actually an online payment gateway solution, which targets the business market or the B2B market in the country and “Hapan” is targeting the kids’ segment in the market.
Privacy theme		
	As per your knowledge, How do you define 'Privacy'?	I would define privacy as actually the user's right to stay away from exposing their personally identifiable data or their details about their personal life and activities
	Have you faced any difficulties when understanding privacy concepts and requirements?	In terms of difficulties, it depends on the focus. So initially in our products, we didn't pay much attention to the privacy aspects. But eventually we even had to face some privacy related incidents as well. As a result of those incidents, we paid a huge amount of focus to embed privacy into our product design itself. I personally did research on privacy and privacy related topics so that we can incorporate those into our software products. So, after doing the research part of privacy and how we should ensure privacy and how we can embed into our products, I didn't have much of a difficulty in understanding the privacy related requirements. The only thing is previously we didn't have a data protection act in the country, so we basically had to gain the base understanding from GDPR from EU. But when the Personal Data Protection Act was introduced to the country, I got access to the draft version. With that I got a clear understanding of what we must do in the roles of data controllers and data processors.
	Are you involved in implementing privacy into the software developed by your company?	Yeah. My involvement is not actually coming from the management aspect, but I contribute more as a Product Owner. As I mentioned earlier, I design the strategic plan for our products so that when designing the product itself, we now consider the privacy aspects. Areas like what are the personal data that we collect, how we are going to store the collected data and how we can avoid any exposure, how we ensure the data security. So that design stage itself now we are embedding the security aspects to our products. But previously the case was different. Our company faced a data breach in 2022. That security attack resulted in exposing data. Back then we didn’t pay much attention to the privacy aspect from the designer perspective. But after that unfortunate incident we started to pay more and more attention to the privacy aspect from the design stage. Even though the incident caused us damage we had a huge amount of learning out of it. Right now, we are practicing all the necessary efforts to ensure the privacy and data security of our all our products.
	What does your company do to ensure that the right privacy protection practices are in place?	In terms of the management perspective, we should ensure privacy and the compliance to the law specially to the Personal Data Protection Act and other related laws that we might need to comply accordingly. But more from a Product Designer perspective, it's more than compliance with the privacy related laws. We look into the integration of privacy in order to achieve the management goal of ensuring privacy and compliance. Therefore, I need to play both roles.

Sri Lankan data protection law theme		
	Are you familiar with the PERSONAL DATA PROTECTION ACT, No. 9 OF 2022? If yes, can you briefly explain.	Yeah, I was aware of the act even before the draft bill was passed through the parliament. Since we are handling a huge amount of personal data through our products and services, ICTA officers who were in charge of drafting the bill contacted me to get my viewpoints related to certain areas. From that involvement I got the exposure and I heavily studied this topic. Considering the time, I won't go into much detail now. In my opinion, the act has covered most of the necessary aspects of how to ensure use of privacy and data security. Act has mentioned about the role of Data Controller and Data Processor. As a company we are acting as the Data Processor for our products. For an example let's take our Helakuru product, we have control over what sort of data to be collected from the end users and how we are going to process the data. But when we lok at our Payhere product, it's a different story. Actually, the business party or the merchant is collecting the customer data and we are acting as the Data Processor for them. When the merchant passes us the collected data we process the data as the payment service provider for that merchant. So that our actual role is the Data Processor. So, in terms of Data Processor, that means the entity or the individual that processors personal data on behalf of the Data Controller. So basically, the data processor needs to fulfil the obligations as specified in the act. When it comes to the obligations of the Data Controller the act mentions a few special points like the consent of the end user. It's important to obtain the consent of the user whenever personal data is collected and then the limitation of the purpose. Only collect the data for the for the specific needs or for the specific requirements and only collect the minimum data needed for the purpose. The data security side covers areas like how to ensure that there are no any unauthorized access or unauthorized intrusion for alteration of the data which is in transit or in storage. When processing the data we need to ensure the integrity of the data in terms of data security and the rights of individuals. If someone doesn't want to give their data to a specific purpose, then need to ensure their right to retain from providing his or her personal data is protected. For cross-border transfers are important when it comes to global product or a service, then how a person's data is accessed from entities outside the country likewise. So those are a few important points that I could recall from the Personal Data Protection Act.
	Are you aware that there are certain Technical and Organizational Measures (TOM) that need to be considered when designing, developing, and implementing software to process personal data? If yes, can you comment on that?	Yeah, as I mentioned previously after the security incident that we faced we are carefully considering both relevant Technical and Organizational Measures. We believe that meeting these measures can enhance the security as a whole.
	PERSONAL DATA PROTECTION ACT, No. 9 OF 2022 states that data	Actually, we are taking all steps to encrypt the data that is stored in our databases.

	encryption and pseudonymization as appropriate Technical and Organizational Measures (TOM), Do you have any work experience concerning these Technical and Organizational Measures (TOM)? If yes, can you briefly explain your experience with that?	Because before that security incident, we only encrypted the passwords when we stored the data in our databases, but not the other customer's personal data. After the data breach, most of the personal data was exposed because of that. As a result of that we took measures to encrypt all the personal data when storing it in our databases. The encrypted data is stored in the databases in different formats and only when those are queried for processing then only, we decrypt and use those.
	Privacy by Design (PbD) theme	
	Are you familiar with the concept called 'Privacy by Design'? If yes, can you point out a few facts that you are familiar with?	Yeah, I'm aware of the concept of Privacy by Design an at the moment, we are practicing privacy by design concept in our company. So, when a new feature of a product or a new product is designed, we ensure the privacy is integrated from the designing stage itself. Previously we didn't practice like that but after the incident we changed to incorporate privacy starting from the design level.
	Are you aware of the seven foundational principles of Privacy by Design? If yes, can you comment on the seven foundational principles.	Yeah, I do and we are following these principles when incorporating privacy into our product development.
	Privacy as the Default is one of the seven foundational principles of Privacy by Design and it means the maximum privacy protection should be provided to the users as a baseline. Can you recall any implementation done by your company that relates to this principle?	So, Privacy as the Default, let's look at an online credit card payment. As the data processor we are receiving certain data of the credit card, for example the name of the card holder, expiry date and so on. Just because we receive all those data, we are not storing all that. We are storing the data which is crucially needed for business purposes only. This is how we follow data minimization in our default setting.
	Embedding privacy theme	
	When you are developing a new software in your company, at which stage of the Software Development Life Cycle (SDLC) privacy is considered?	Before the security incident that we faced, we considered security considerations like privacy just as another requirement that we will pay attention in the development stage. But at present our approach is different, we have a separate Security Team who will take part in the software development life cycle from the design level itself.
	Can you provide examples of specific practices or strategies your company follows to integrate privacy by design principles into the Software Development Life Cycle?	One step we took is introducing a Security Team in which the team members are specialized and have the knowledge related to not only security tools and all but also privacy by design concepts as well. We do encrypt all data saved in our databases and we will decrypt only when it is needed to be processed. When it comes to access controls, those were implemented from the beginning itself. We provide role-based access. For example, there are roles like Marketing Level roles, technical roles and Customer Service Level roles. so based on their levels necessary user accesses are being granted. I guess about data minimization I mentioned ealier as well. Now we collect and store data which is cruicial and required to process business purposes. Another important practice that we introduced lately was regarding Audit trials and Logs. Earlier we used to store the Audit trails and Logs in the same servers that we store data. But now we use a third-party service provider to store our Audit trails and Logs separately. I'm working closely with security consultants these days, because we are planning to get some International certifications so we are in the middle of revamping some internal processes as well.

	Do you think there is a trade-off between implementing core functionality and embedding privacy in the design? What is your perception of this?	Exactly, there is a trade-off. You know I can understand it well since I work on both the product design level and then in the UX aspects. When we increase the security with all these security measures, then the user experience can go down. But when we improve the user experience, then the level of security will not be that strong. So that is how I actually experienced the trade-off. Most of the time our main focus was to provide a simple solution which a non-tech savvy person can easily adapt to. So, when building a simple solution as such user experience matters and we deviate from the privacy aspects. But after the data breach incident, we always try to maintain the balance between those two. Our aim is to build a solution which can give a good experience to the end users while ensuring privacy. In reality, when balancing this we need to have discussions all the time with product consultants and security consultants. This is something we need to manage in an ongoing manner while continuously improving.
	In your work setup, who is held responsible for embedding privacy to the technology design of a software?	We have a dedicated security team but that doesn't mean it's their responsibility only. As a Product Owner and UX Designer I myself contribute accordingly to ensure that the right privacy measures are embedded to our products. So this is a team effort, I believe.
	What is the nature of the stakeholder collaboration when embedding privacy in to the Software Development Life Cycle?	Like I told you before, making privacy a part of the software is a team effort. Security Consultants are not the only ones to be held responsible, but also legal teams, developers, marketing team and clients as well. I play different roles, but I always make sure to pay attention to privacy concerns and security aspects. Not only that from the management perspective, also I discuss with our customers to make alignments regarding privacy and all.
	How does your company ensure that you and your team have the necessary knowledge and skills to implement privacy by design effectively?	Through self-learning and by exploring the Personal Data Protection Act and GDPA, I learnt a lot. But our employees are going through formal training with the Security Consultants.
	Assuming that you are given a chance to take an initiative for the integration of privacy into the software development lifecycle or to enhance the current practices, what would be your approach?	You will not understand the importance of security until you face an unfortunate security incident. Since I have gone through that now I know how important this privacy in the software development process is. So if I'm given a chance to do this all over again. I will give the needed level of priority to embed privacy from the design stage without compromising the user experience of the end users. Whatever the new practices that we introduced recently, I would incorporate those from the start itself.
	Have you observed any specific examples or case studies where the integration of privacy by design has had a significant impact on the success or failure of a software development project? If so, would you like to share an example or a case study?	Actually, I spoke about the data breach that we faced throughout the interview so that is the real use case that I can tell you that I experienced myself. While answering some of your earlier questions I told you about what we didn't do and what practices we implemented later on and how we see benefits out of those. This incident actually showed a new direction to our company and with that we were able to improve our products and still we are continuing to do so. In this industry, sometime we cannot prevent bad incidents entirely. But, if we manage to learn quickly and correct the mistakes on privacy we made in the past, we will be known as a trustable software developer. It is important that we pay attention to the incidents of other players, and realize it could happen one of our developed software too. So, we check for the possibility of such event with our developments and make neccesary action, before it occurs.

	"Embedding privacy into the technology design will allow the company to gain a competitive advantage" What is your perception on this statement?	I totally agreeing with this. We will be partnering with an AI Tech Company to proactively identify and avoid the fraud payments through the payment gateway. This is going to cost us a lot but having an AI powered fraud detection facility for our solution will definitely add a competitive advantage. So, at the moment we are working on this initiative. This is how we see privacy as something that can help us to gain competitive advantage.
Closure		
	Do you want to add anything relevant to the subject that we have not discussed during this interview?	We discussed a lot during the interview. Nothing from my side to add other than giving the final message of how important the security in a software is. It was a pleasure to be a part of this study. Thank you.
[Thanking for the participation]		

Transcript 7

	Question	**Answer**
Introduction		
	First of all, do you mind if I record this interview?	Yeah, that's fine.
[Introduction to the study]		
[Statement that conveys the confidentiality and data usage aspects]		
	Can I use your name and the company that you are working for? Or else do you wish to provide a pseudonym or stay anonymous?	You can use my name and designation. Sanduni Wickramasinghe: Legal Consultant - Information Privacy & Technology Law
	Can you please briefly describe your work experience in the Sri Lankan software development industry?	I started my career about 10 years ago working for the government in the intelligence department, focusing on matters related to Ceypetco. After that, I spent nearly five years with Mobitel, where I was part of the internal legal team. Since then, I've ventured into my own consulting practice, which I've been running for about two and a half years. My primary focus in consulting is on technology law, with a special emphasis on data protection, privacy, and digital rights.
	What is your current job role, and what are your responsibilities?	In my current role, part of my portfolio involves advising companies on implementing data protection frameworks within their organizations. This includes guiding clients on the regulatory framework in Sri Lanka concerning personal data processing and advising both local and international companies on their privacy regulatory landscape. Additionally, I was a member of the Personal Data Protection Act drafting committee from early 2019 until its completion in November 2021.
	What is the nature of the software designed by your company?	Most recently, I provided informal consultancy to the World Lab. In my previous roles, I worked on various customer-facing applications that involved handling personal data of subscribers. Currently, I advise companies on the use of tracking software, particularly where processing personal data and

		improving location data are involved. Additionally, I provide regulatory advice to a social media company, focusing on usage and compliance issues.
	Privacy theme	
	As per your knowledge, How do you define 'Privacy'?	I believe privacy is a notoriously difficult term to define, as different scholars have varying interpretations. For me, privacy, particularly information privacy, is about having personal autonomy over what information is disclosed and maintaining control over one's own information. While privacy encompasses various aspects like physical and territorial privacy, information privacy, in my view, centers on having that sense of control and autonomy over one's personal data. On the other hand, Privacy is also about the steps taken to ensure the Privacy of person, such as implementign access controls, or putting limitations for the type of data that will be collected.
	Have you faced any difficulties when understanding privacy concepts and requirements?	My academic training, including postgraduate studies focused on this area of law, has helped me understand the nuances and implications of privacy. Additionally, being a certified Information Privacy Professional and staying updated with certifications from the International Association of Privacy Professionals has kept me informed about the evolving privacy landscape. This ongoing education and certification have aided my understanding of the changing nature of privacy concepts and requirements, both locally and globally, and have helped me navigate these complexities without facing significant difficulties.
	Are you involved in implementing privacy into the software developed by your company?	Currently, my main focus is on formulating privacy policies, typically occurring after the software design is complete. Often, clients approach me when they're about to launch their software and realize they need a privacy policy. Unfortunately, privacy policies are sometimes viewed as a mere compliance formality. My role involves mapping out the personal data involved, analyzing data flows, and advising on how to process this data in accordance with the applicable legal framework.
	What does your company do to ensure that the right privacy protection practices are in place?	In Sri Lanka, the constitution does not explicitly recognize the right to privacy, and the courts have not formally acknowledged it as a fundamental right, unlike in some other jurisdictions. Although privacy is referenced as an exception to the right to freedom of information, it is not explicitly recognized. The Personal Data Protection Act (PDPA) provides some statutory rights related to personal data, but it does not fully address privacy concerns. In advising companies, I focus on ensuring compliance with the PDPA, which mandates proper handling of personal data according to principles like lawfulness, specification, and communication. I also emphasize the importance of implementing mechanisms to uphold rights such as access to information. Even without a constitutional right to privacy, my general advice is for companies to align their practices with the requirements of the PDPA to ensure proper data handling and protection.

Sri Lankan data protection law theme		
	Are you familiar with the PERSONAL DATA PROTECTION ACT, No. 9 OF 2022? If yes, can you briefly explain.	I believe the PDPA, which came into effect in early 2019, was introduced to address key issues like the need for a legal framework supporting government and private sector data handling amidst growing digitization and cross-border data processing. It aims to provide a safety net for individuals in Sri Lanka and align with global trends in data protection.The Act sets out principles for processing personal data, including lawfulness, purpose justification, accuracy, confidentiality, and transparency. It defines roles such as controllers, processors, and data subjects, and has extraterritorial application, meaning it also covers entities targeting the Sri Lankan market, like social media platforms and e-commerce sites.The PDPA grants data subjects new rights, such as the right to withdraw consent, access, erasure, rectification, and review decisions made through automated processes. It also establishes a Data Protection Authority to enforce the Act and includes provisions for cross-border data flows, data protection assessments, and the appointment of data protection officers. Drawing from international standards like GDPR and OECD guidelines, the PDPA aims to provide a comprehensive framework for data protection in Sri Lanka.
	Are you aware that there are certain Technical and Organizational Measures (TOM) that need to be considered when designing, developing, and implementing software to process personal data? If yes, can you comment on that?	In my view, the Act first addresses the obligation to maintain the integrity and confidentiality of personal data. It requires every controller to use appropriate technical and organizational measures like encryption, pseudonymization, anonymization, and access controls to protect personal data. The Act also allows the Data Protection Authority to prescribe additional TOMs in the future to prevent unauthorized processing and protect data from loss, destruction, or damage. Under Section 21, controllers must ensure that any processors they use also have appropriate TOMs to meet the Act's requirements and protect data subjects' rights. This means controllers need to assess the TOMs of any third party they outsource data processing to. This requirement should be part of the due diligence process during RFP assessments. Section 22 adds that processors must also have appropriate TOMs and ensure their personnel are bound by confidentiality obligations when handling data for controllers. Even though the Act doesn't specifically mention TOMs in software design, development, and implementation, I believe the holistic view of the Act implies that controllers must have necessary TOMs to fulfill their obligations, especially under the accountability requirement in Section 12, which calls for a data protection management program. Thus, it's clear that having TOMs in place is essential for meeting the Act's requirements.

	PERSONAL DATA PROTECTION ACT, No. 9 OF 2022 states that data encryption and pseudonymization as appropriate Technical and Organizational Measures (TOM), Do you have any work experience concerning these Technical and Organizational Measures (TOM)? If yes, can you briefly explain your experience with that?	In my experience, encryption and anonymization aren't always used, particularly when it comes to technical and organizational measures (TOMs) for protecting personal data. While encryption might not be widely implemented, access controls and other measures are commonly used. In one case, I saw anonymization applied because the data was aggregated and stripped of identifiers to meet a business requirement rather than compliance needs. This shows that the use of TOMs can vary based on organizational requirements. Generally, encryption isn't always used due to its cost, but for highly sensitive information, like health data, encryption might be used as an additional precaution.
Privacy by Design (PbD) theme		
	Are you familiar with the concept called 'Privacy by Design'? If yes, can you point out a few facts that you are familiar with?	So, I think it was initially coined by Martin Cavokian, the Canadian commissioner in the data protection office in the 1990s, I guess, if I remember it right. And then this has been something that has been highly common in the health community. And you see references made to it in the EU General Data Protection Regulation as well. So there is actually a specific requirement to make sure that controllers embrace or implement PbD principles of privacy by default. So as far as I'm aware, there are seven principles there, and it goes on to explain how you can balance the, you know, privacy against the business requirements and operational requirements. Because one of the biggest criticisms of having privacy regulations, I mean, this is something even the Sri Lankan, when we were drafting it, the level against the introduction of such a law was that this is going to inhibit innovation and it's going to be a costly affair and whatnot. But if you look at the different principles and the PbD, you will see it's not a zero-sum approach, but it can work as a positive-sum approach. And you know that you need not have, hand over your privacy for the sake of security, but here is something that can be achieved as a win-win situation. So, I think the misconception when it comes to privacy laws is essentially that people don't understand, you know, how privacy can actually be worked into their system, worked into their processes and all that. And I think we advise you to think about it from the very inception. I think this is something or think about these principles from the very early design stage. I think it's something you can effectively achieve without compromising your business requirements or your innovation or your operational needs.
	Are you aware of the seven foundational principles of Privacy by Design? If yes, can you comment on the seven foundational principles.	Yes, I am aware of the seven foundational principles of Privacy by Design. These principles advocate for proactive privacy measures, ensuring that privacy is embedded into the design of systems from the start, rather than being added later. They emphasize that privacy should be the default setting, with strong security measures in place throughout the data lifecycle. The principles also highlight the importance of creating systems that balance privacy with functionality, maintaining transparency about privacy practices, and respecting user privacy in all aspects of design and operation. This approach aims to integrate privacy seamlessly into both technology and business processes.

	Privacy as the Default is one of the seven foundational principles of Privacy by Design and it means the maximum privacy protection should be provided to the users as a baseline. Can you recall any implementation done by your company that relates to this principle?	In my experience, achieving privacy by default often starts with minimizing data collection. For instance, when collecting data, such as in a survey or any other context, I advise clients to only gather information that is strictly necessary for the intended purpose. In many cases, I've noticed that asking for unnecessary details, like physical addresses or personal identification numbers, can be counterproductive and doesn't serve a clear purpose.By focusing on data minimization, I believe privacy by default can be effectively implemented. This means from the outset; you should question the necessity of each piece of information you're collecting. If it doesn't directly contribute to achieving your objective, it's best not to collect it. This approach not only helps in meeting privacy requirements but also reduces compliance risks and protects individuals' privacy more effectively.
Embedding privacy theme		
	When you are developing a new software in your company, at which stage of the Software Development Life Cycle (SDLC) privacy is considered?	At the very initial design stage of developing software, I believe it's crucial to consider privacy concepts. For example, when developing an application, I need to evaluate why certain information, like contact details or access to photos, is needed. Different stakeholders, such as marketing and sales teams, may push for extensive data collection, while legal and regulatory teams will be more cautious. It's important for me to address these privacy concerns early on because incorporating them later can be challenging. Balancing the needs of various business units and mitigating pushback from teams focused on sales and marketing can be difficult, but discussing privacy frameworks from the start can help manage these issues effectively.
	Can you provide examples of specific practices or strategies your company follows to integrate privacy by design principles into the Software Development Life Cycle?	To integrate privacy by design principles, our company involves various stakeholders, including marketing, sales, legal, and regulatory teams, from the very beginning of the software development process. We ensure that privacy considerations are discussed and addressed early, rather than embedding them later, which can be difficult and lead to resistance from different departments. For example, while marketing and sales teams might push for more data collection to drive sales, the legal and regulatory teams ensure that data usage complies with privacy regulations. By involving these different perspectives early, we mitigate potential pushback and balance the needs of all stakeholders effectively.
	Do you think there is a trade-off between implementing core functionality and embedding privacy in the design? What is your perception of this?	When implementing privacy measures, the timing can influence the process. If it's at the latest stage of development, I might face trade-offs. However, I believe that Privacy by Design should not involve trade-offs if I integrate privacy protection from the beginning. By embedding privacy into the strategy and development process, I can often meet both business needs and privacy concerns without compromising one for the other. I advise clients not to view privacy compliance merely as a checklist but as a tool to build and maintain consumer trust. In a market where personal data is crucial, establishing and sustaining trust is essential, especially as consumers become more aware of privacy issues. For example, the reaction to Facebook's changes to WhatsApp's terms and the shift towards platforms like

		Telegram or Signal highlight the growing importance of privacy. If my vision includes prioritizing user privacy, I don't think I will face a true trade-off between privacy and business objectives.
	In your work setup, who is held responsible for embedding privacy to the technology design of a software?	I believe that there's a misconception that privacy and legal compliance are solely the responsibility of the legal team. In my view, organizations need to invest in educating and raising awareness among their technical teams as well. Often, products are conceived by non-legal teams, such as marketing or IT. If these individuals, including executives who drive product strategies, understand privacy issues and risks, it becomes a shared responsibility rather than being confined to one division. Everyone should be aware of legal compliance, consumer trust, and transparency. While there might be a designated role like a Data Protection Officer (DPO) for organizations processing large amounts of data, I think privacy should be integrated into the organization's culture for it to be truly effective.
	What is the nature of the stakeholder collaboration when embedding privacy in to the Software Development Life Cycle?	I believe it's crucial to involve the legal or regulatory team from the very beginning when designing software. Their expertise helps me understand the legal requirements, reducing the company's exposure to fines, penalties, and compliance risks. Including them early on ensures that we address legal and regulatory aspects before the product is launched, avoiding delays from separate assessments later. This collaboration, along with input from marketing and other stakeholders, helps me align everyone's requirements and develop a solution that meets business needs while minimizing disruptions.
	How does your company ensure that you and your team have the necessary knowledge and skills to implement privacy by design effectively?	I would start by helping them understand the law and its legal requirements. Then, I would discuss their business needs with them to figure out how to meet each of the principles and requirements. For instance, when it comes to data retention, I'd gather information on how long they need to keep the data and whether there are any legal requirements for longer retention. I would then advise on how to determine the appropriate retention period based on their needs and legal obligations. Essentially, my approach involves having open conversations with both technical and business units to understand their requirements and then guiding them on how to comply with legal obligations.
	Assuming that you are given a chance to take an initiative for the integration of privacy into the software development lifecycle or to enhance the current practices, what would be your approach?	In the early stages of design, I map out the personal data requirements and data flows to understand what data is needed and its purpose. I create an inventory of these personal data requirements and then evaluate each principle to ensure it meets the regulatory framework without negatively impacting business operations. Additionally, I compare the personal data requirements and proposed technical infrastructure against data subjects' rights to ensure those rights can be effectively enforced if necessary. This is my general approach when advising an entity on integrating protection principles into their software from the beginning.

	Have you observed any specific examples or case studies where the integration of privacy by design has had a significant impact on the success or failure of a software development project? If so, would you like to share an example or a case study?	That's a bit tough one. So currently I'm working with one startup but it's yet to, so I'm just advising them on so I'm yet to see proofs of that. But the thing is when you are a consultant you end up, I mean you provide a consultation and come to the client who decides whether they you know embedded it or not. So, I actually don't have much visibility to how the you know eventual product was designed so I don't think it's a question I can fully answer right now.
	"Embedding privacy into the technology design will allow the company to gain a competitive advantage" What is your perception on this statement?	I would say yes because one, it reduces your risk of compliance and effectively helps reduce the risk of data breach if designed properly. It depends on the context in which they operate. Still, if it's something that expects individuals to share more and more personal data with them, I think the more you, not just portray but position yourself as a privacy-conscious organization, the more customer base you will be able to grow. And in addition to that of course, like I said this will reduce your risk of not just compliance but also data breach risk if you know if you're adhering to security by design and privacy by design. So then I think it's safe to say that an organization will stand to achieve a competitive edge compared to their competitors in particular if they are a privacy-conscious entity or a product compared to their competitors. Because the more, I mean the less risk profile you would have in this in terms of personal data, I believe that would add to having a competitive edge over your competitors. So, I don't think there's any trade-off in terms of, or you reside in a trade-off between giving up your operational needs over to achieving or meeting any regulatory or compliance needs.
Closure		
	Do you want to add anything relevant to the subject that we have not discussed during this interview?	We discussed a lot during the interview. Nothing from my side to add. It was a pleasure to be a part of this study. Thank you.
[Thanking for the participation]		