AN EU – GDPR BASED PRIVACY ASSURANCE FRAMEWORK FOR DATA PROCESSORS IN SOFTWARE PACKAGE IMPLEMENTATION INDUSTRY IN INDIA

by

Premnath Rajagopalan, MBA

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

<November, 2025>

AN EU – GDPR BASED PRIVACY ASSURANCE FRAMEWORK FOR DATA PROCESSORS IN SOFTWARE PACKAGE IMPLEMENTATION INDUSTRY IN INDIA

by

Premnath Rajagopalan

APPROVED BY

Dissertation chair

RECEIVED/APPROVED BY:

Renee Goldstein Osmic

Admissions Director

Dedication

"Believe in yourself when nobody else does." — Mary J. Blige

“Perfection is not attainable. But if we chase perfection, we can catch excellence.” — Vince Lombardi

I would like to express my heartfelt gratitude to my parents, family, and friends, whose unwavering love, support, and encouragement have been a constant source of motivation and inspiration throughout my academic journey. Their support has been invaluable in helping me overcome any obstacles, and their motivation has shaped both the person and the learner I have become.

I would also like to acknowledge my mentor, Prof. Dario Silić, PhD, who has been an invaluable coach and advisor throughout my research. His expertise, feedback, patience and constructive criticism have been instrumental in honing my research skills, and I am grateful for the opportunity to learn from him. His mentorship has helped me become a better researcher and scholar and has played a significant role in shaping my academic and professional journey.

Acknowledgements

Acknowledgments are an essential part of the thesis as they allow me to express gratitude to those who have contributed to completing this work. First and foremost, I would like to thank God for providing me with the strength, wisdom, and perseverance needed to complete this research.

I would also like to take this opportunity to acknowledge and express my sincere appreciation to the following individuals and teams who have supported me throughout the completion of my thesis.

I am deeply grateful to my thesis mentor, **Prof. Dario Silić, PhD**, for his invaluable guidance, support, patience and encouragement throughout my research journey. His expertise and feedback have been instrumental in shaping my ideas, refining my arguments, and improving the overall quality of my work. I am genuinely thankful for the time, effort he has invested and his unwavering support during the challenging times.

Furthermore, I would like to thank all colleagues and friends who have provided a stimulating academic environment and valuable feedback on my work. Their contribution in completing the survey and their encouragement have kept this process motivated and focused throughout the research journey for this paper.

I am especially thankful to my family for their unwavering support, encouragement, and sacrifices throughout my academic journey. Their love and support have been my source of strength, and I am grateful for everything they have done.

I would also like to thank the Swiss School of Business Management for allowing me this opportunity to explore the possibility of research and supporting me this thesis. The school's efforts and guidance have been essential in completing this journey.

I am deeply indebted to all the individuals and teams mentioned above for their support, encouragement, and assistance throughout my research journey. Their contributions have been critical in ensuring the successful completion of my thesis, and I am profoundly for their unwavering support.

ABSTRACT

AN EU – GDPR BASED PRIVACY ASSURANCE FRAMEWORK
FOR DATA PROCESSORS IN SOFTWARE PACKAGE
IMPLEMENTATION INDUSTRY IN INDIA

Premnath Rajagopalan
2025

Dissertation Chair: Aleksandar Erceg, PhD

In the ever-changing landscape of data protection and privacy regulations, exemplified by the EU General Data Protection Regulation (EU-GDPR, Regulation (EU) 2016/679), Indian data processors within the software package implementation sector face significant compliance challenges.

This study aims to report these challenges by emerging a tailored privacy assurance framework, finely tuned to the unique context of package implementation in India. This research reveals the gaps or limitations in the Digital Personal Data Protection (DPDP) Act in India as a second best solution for software package implementation sector but also proposes a new framework with standards as a first best solution in order to be in full compliance with the market expectation from the globalized clients, mainly from EU regarding the data protection and privacy regulations in the globalized economy which is subject to constant technological changes. In a globalized economy subject to constant technological changes, meeting these regulatory expectations becomes imperative.

India's software package implementation sector plays a pivotal role globally, contributing nearly 8% to the nation's GDP during 2017-2018, has grown to account for 11% during 2021-2023. Making it a formidable player in global IT arena. The sector's dominance, holding 55% of the global IT outsourcing share, underscores the essential for a strong data protection framework, with the EU-GDPR emerging as a potential benchmark. The substantial contribution of the IT sector to India's GDP emphasizes the paramount need for a strong data protection framework.

However, the emergence of stringent rules like the EU-GDPR and the DPDP Act has brought data security and privacy issues into sharp focus for Indian software package companies, functioning as data

processors. Indian data processors now grapple with the intricate task of aligning their local corporate practices with the EU-GDPR and DPDP Act requirements while serving European clients. This research adopts a multifaceted approach, incorporating a comprehensive literature review, surveys targeting Indian software package organizations, and in-depth interviews with key department stakeholders. The survey encompasses various departments within these organizations, including Legal, HR, administration, and IT. Additionally, the plan is to include overall data on the percentage of GDP contributed by the surveyed companies which make it crucial impact on the need for data privacy for these organizations.

This research anticipates yielding valuable understandings into the current state of GDPR and DPDP Act compliance amongst Indian companies functioning as data processors. The focus is on identifying areas of merging and separation between EU-GDPR and DPDP Act standards and prevalent Indian privacy practices. Furthermore, this research aims to present a meticulously tailored privacy assurance framework designed to bridge these gaps and facilitate compliance with the EU-GDPR and DPDP Act, particularly for data processors in the Indian software package execution sector.

The findings will be discussed in the background of privacy and data protection in India's software package implementation industry. The proposed framework will undergo detailed evaluation to determine its feasibility and effectiveness in addressing compliance disparities and challenges. The study will also cover on the potential challenges and advantages associated with implementing such a Privacy Framework.

This research presents a comprehensive strategy for addressing the intricate challenges related to data privacy and protection compliance encountered by software package implementers in India. By crafting a privacy assurance framework tailored to the Indian context, this research aims to identify the necessary data security measures within the scope of the EU-GDPR considering also DPDP Act. These measures can be adopted by Indian companies to achieve compliance with EU standards, ultimately enhancing the sector's competitive edge, fostering quality standards in data protection, and ensuring business continuity and profit generation.

Keywords: EU-GDPR, Data Protection, Data Processors, Privacy Assurance Framework, Software Package Implementation in India, DPDP Act, Data Security, Compliance, Client Data Protection.

TABLE OF CONTENTS

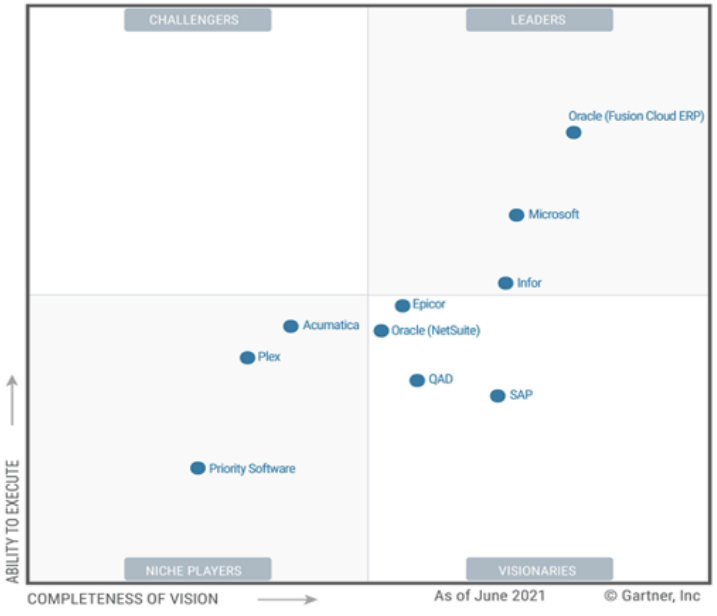
CHAPTER I: INTRODUCTION

This chapter introduces the research background, outlines the core problem of GDPR compliance for Indian software package firms, and sets the foundation by defining the objectives, motivation, significance, and key questions guiding this study.

1.1 Introduction

A company's strategy, structure, as well as culture can be significantly shaped by an enterprise system. However, these systems come with a set of risks that should not be overlooked (Davenport, 1998). According to Alter (1999), ERP systems are information systems that use a unified database to facilitate a range of business processes within functional areas and maintain consistency across operational areas of a business. Typically, ERP packages consist of various units that can be selected and implemented independently, depending on the specific requirements of an organization. These ERP implementations provide custom-made and out-of-the-box packages that can accommodate different business critical modules, such as production planning, materials management, sales & distribution, capital management, customer relationship management, finance management, as well as data analytics monitoring, across various industries, including manufacturing, healthcare, human resources, and much more. Customers worldwide usually prefer cloud-based package software providers such as Oracle, Microsoft Dynamics, and SAP as their most preferred ERP packages, (Gartner, 2021) (Davidson, 2023)

Figure 1:Magic quadrant for product centric Enterprises.



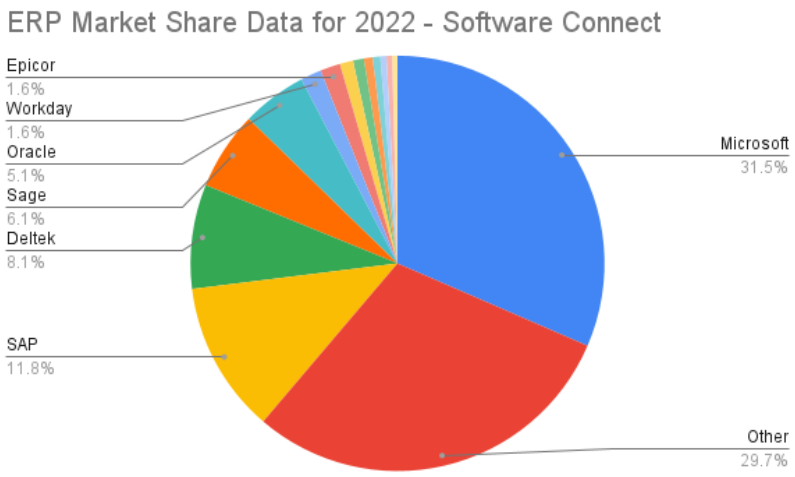
Source:(Gartner, 2021**)**

In most of the instances of package implementations, the development and deployment for customers is done by preferred partners of package providers who operate in onsite-offshore based model in multiple regions across the globe. Some examples to quote on onsite-offshore model package implementation with offshore delivery centre in India are:

1. A preferred partner for Microsoft dynamics Package in Europe region collaborating with offshore delivery centre in India for customer implementation.
2. A preferred partner for Oracle Fusion suite package in United Kingdom region collaborating with offshore delivery centre in India for customer implementation.
3. A preferred partner for System analyse Programmetwicklung (SAP) suite package in North America region collaborating with offshore delivery centre in India for Customer implementation.

When it comes to complying with the GDPR, the majority of organizations that use an onsite-offshore model and operate in different areas for businesses established in the EU are still unprepared. To lessen liability under the GDPR, organizations about the world are developing changes on their operational approach to be in compliance with the GDPR and its implications towards Data Security across borders. India's IT sector, which contributed nearly $177 billion in revenue and constituted almost 8% of the nation's GDP during 2017-2018, has grown to account for 11% during 2021-2022, making it a formidable player in the global IT arena (Ministry of Statistics and Programme Implementation, 2021). Its dominant position, commanding 55% of the global IT outsourcing market, accentuates the urgency for a robust data protection framework, with the EU General Data Protection Regulation (EU-GDPR) serving as a potential benchmark (The BPO Network, 2022). Based on recent market reports, Davidson (2023) states that the software package implementation industry in India has observed important growth in recent years and has emerged as a vital sponsor to the country's economy.

Figure 2:ERP Market Share Data



Source: Davidson, 2023

The significant expansion of enterprise packages has also posed new challenges, particularly concerning privacy and data protection (Davidson, 2023). The introduction of the EU GDPR has led to higher demand for robust data protection measures, which presents new challenges and potential opportunities for organizations worldwide to improve their data security. The GDPR of the European Union has created a stringent standard for ensuring privacy in the management of personal data, setting a benchmark for privacy protection globally (Vranaki, 2016). As the software package implementation industry in India continues to expand, there is an escalating need for a privacy assurance framework that adheres to the principles of the EU-GDPR.

1.2 Research Problem

Indian software package implementation organizations processing data for EU clients as data processors face significant challenges in complying with GDPR (Gupta and Joseph, 2020). The GDPR has set an ambitious target for data protection, requiring organizations to implement comprehensive privacy frameworks that confirm agreement with GDPR's stringent needs. The lack of established guidelines and regulations for a data protection framework in India and the complexities of cross-border data processing pose legal, ethical, and operational challenges (Lekhi, 2021a). This has left many Indian data processors vulnerable to potential non-compliance penalties and operational difficulties serving EU Clients. This research aims to identify these challenges as well as develop an adaptive privacy outline for Indian data processors in software package implementation, facilitating smoother compliance with GDPR and upcoming DPDP act.

1.3 Research Objectives

The investigate aims to assess the implications of data protection compliance for Indian software package implementation companies, focusing on developing a comprehensive outline that aligns with the GDPR while also incorporates the key areas of the DPDP Act. The primary objective is to enhance data protection compliance within the Indian software sector, particularly among companies serving European Union (EU) clients. By examining the challenges associated with GDPR, the study intends to propose an adaptive privacy assurance framework that not only addresses the unique requirements of Indian data processors but also ensures that core aspects of the DPDP Act are integrated. This dual approach is designed to close existing gaps in India's data protection landscape, offering a structured method for achieving both GDPR alignment and DPDP adherence. The goal is to provide Indian companies with the necessary tools to achieve compliance with global and local data protection standards, thereby strengthening their overall data protection practices and boosting their competitiveness in the international market. This aligment seeks to address existing compliance challenges and improve India’s data protection standards through a holistic framework (Greenleaf, 2020).

1.4 The Research's Importance

This research has significant implications for India’s growing IT sector, particularly the software package implementation industry, which serves as a critical contributor to the country’s GDP. Ensuring acquiescence with global data protection rules, such as GDPR, is essential for maintaining the industry’s international reputation and competitiveness. Moreover, alignment with GDPR will help Indian companies build trust with EU clients, foster stronger business partnerships, and ensure the protection of sensitive personal data (Davidson, 2023). Furthermore, the study emphasizes the importance of developing a comprehensive data protection framework in India that not only aligns with international standards but also reports the specific requests and challenges of Indian data processors.

Aligning the DPDP Act with GDPR standards is vital for improving data protection practices in India and maintaining global competitiveness. This investigation offers insights for policymakers, businesses, and stakeholders on improving data protection measures and strengthening client trust (Clarke et al., 2018, Shekhar and Choudhary, 2022).

1.5 Purpose and Research question

Given the complexities of cross-border information processing and imperative for robust data protection frameworks in India, this research focuses on investigating the challenges Indian software package implementation organizations face in complying with GDPR while processing data for EU

clients is crucial. This study does not aim to propose a new regulation or legal policy, but rather to develop a GDPR-compliant privacy assurance framework a structured, practical methodology combining operational processes, compliance best practices, and selectively adapted GDPR and DPDP Act elements. This framework is designed specifically for Indian software package implementation firms to follow internally, enabling them to meet international expectations without relying on new legislation. The key research questions driving this study are:

- **RQ1:** What are the key challenges faced by Indian software package implementation organizations in complying with GDPR expectations, and can GDPR standards be adapted into a new framework with Indian specificities?
- **RQ2:** To what extent are Indian software package organizations aligning their data processing practices with EU-GDPR and DPDP Act requirements?
- **RQ3:** What legal and compliance challenges do Indian software package organizations face in achieving EU-GDPR and/or DPDP Act compliance?
- **RQ4:** How can a practical privacy assurance framework , based on adapted GDPR and DPDP standards, be developed to support compliance for Indian data processors?

The study's primary goal is to develop a privacy assurance framework that enables Indian software package implementation companies to achieve GDPR compliance while also aligning with the DPDP Act.

1.6 Research Motivation

Enhancing GDPR compliance is crucial for Indian software package implementation companies to maintain trust with global clients and ensure privacy. As the software package implementation industry's contribution to India's GDP grows, understanding GDPR compliance in this context becomes paramount. Non-compliance or inadequate data protection could lead to missed business opportunities, impacting the economic contribution of the industry. Beyond asserting the position of GDPR adherence for data protection in the Indian software industry, this research aims to establish a GDPR-aligned framework that synergizes with India's DPDP, enhancing trust and economic rapport with the EU market. This research will also contribute to strengthening data safety practices as well as ensuring the accountable use of personal data and its security aligned towards Compliance with EU GDPR standard.

1.7 Research Significance

1.7.1 Potential Findings

Based on our first research, it appears that the software package deployment industry in India might benefit from a privacy assurance framework that is based on the EU-GDPR. These findings include:

- Market Access and Trust: Indian data processors specializing in software package implementation may experience improved access and greater trustworthiness in European markets when aligned with GDPR principles.
- Business Partnerships: Implementing enhanced data protection measures can attract preferred business partnerships within India, fostering trust and reliability among stakeholders.
- Economic Contribution: The software package implementation sector is a significant contributor to India's GDP, highlighting the urgent essential for a huge data protection background to ensure GDPR compliance. Table 1 below demonstrates the impact on GDP growth trends and data privacy in India's IT sector.

Table 1: Impact on GDP Growth and Data Privacy

Year	GDP Growth in Indian IT Sector (%)	Reasons for Data Privacy Importance	Impact on Data Protection without GDPR and DPDP Act	Impact on GDP Growth
2015	10.5	1. Protection of sensitive customer information	Limited safeguards, higher risk of data breaches	Negative impact
2016	12.2	2. Compliance with global data protection regulations	Non-compliance, potential legal issues	Negative impact
2017	11.8	3. Enhanced trust and credibility with clients	Reduced trust due to inadequate data protection	Negative impact
2018	13.5	4. Mitigation of data breaches and cyber threats	Vulnerability to cyberattacks and data theft	Negative impact
2019	14.2	5. Facilitation of cross-border data transfer	Hindered cross-border data flow due to privacy concerns	Negative impact

Year	GDP Growth in Indian IT Sector (%)	Reasons for Data Privacy Importance	Impact on Data Protection without GDPR and DPDP Act	Impact on GDP Growth
2020	9.7	6. Avoidance of legal penalties and fines	Potential legal fines and penalties for non-compliance	Negative impact
2021	11.0	7. Protection of intellectual property and trade secrets	Risk of IP theft and trade secret exposure	Negative impact
2022	10.5	8. Ensuring data ethics and responsible data handling	Ethical concerns, potential data misuse	Negative impact
2023	11.0	9. Transition to new legal regime – awareness and preparedness for DPDP Act release.	Weak enforcement mechanisms, continued risk of data misuse and inadequate privacy safeguards	Moderate Impact

Source: (Ministry of Statistics and Programme Implementation (MoSPI). National Accounts Statistics Government of India, 2023)

This structured table provides a clear view of how GDP growth in the Indian IT sector, increasing data privacy importance, and the impact of not having a privacy regulation like GDPR and DPDP Act are related over the years. The impact is considered negative because of the absence of robust privacy regulations during this period led to increased data breaches, weakened international trust, reduced cross-border data flow, and lost business opportunities, all of which indirectly slowed down the growth potential of the Indian IT sector despite its otherwise strong performance and stable revenue.

1.7.2 Key Challenges

Despite its potential benefits, the Indian software package implementation industry faces significant challenges in aligning with GDPR compliance requirements:

- Infrastructure Limitations: Some regions in India experience inconsistent connectivity and unreliable network security, impacting the industry's ability to meet GDPR data protection standards.
- Cross-Cultural Communication Challenges: The need to align Indian implementation practices with GDPR requirements for European clients can result in communication difficulties, data leakage risks, and misunderstandings during project execution.

- Talent Management Complexities: While India has a large IT workforce, selecting the right professionals for data security and privacy compliance remains a challenge, impacting the effectiveness of GDPR implementation.

1.7.3 Strengths of This Research

This study offers several key strengths that contribute to its originality and practical relevance in the field of data privacy compliance.

- Multidisciplinary Approach: By integrating IT, legal, and policy perspectives, the research offers a holistic understanding of GDPR compliance challenges for Indian data processors.
- In-Depth GDPR Analysis: The study provides a detailed examination of GDPR complexities, focusing on specific challenges faced by Indian businesses due to regulatory and operational differences.
- Tailored Framework Proposal: A customized GDPR compliance framework is proposed, addressing industry-specific needs and practical implementation within the Indian software sector.
- Economic Impact Assessment: The research highlights the direct link between GDPR compliance and India's software industry growth, emphasizing benefits such as enhanced global competitiveness and trust.
- Use of Real-World Data: Empirical data is leveraged to reinforce the study's findings, demonstrating the tangible advantages of compliance, including risk mitigation and business sustainability.

The study's qualities allow it to contribute to both theoretical knowledge and practical insights for enterprises, governments, and industry practitioners in India as they navigate and gear up for GDPR compliance.

To Summarise, this chapter highlighted on the background of the research, the main compliance challenges that Indian software package implementation firms face with GDPR and the DPDP Act. It also described the purpose of proposing a practical privacy assurance framework, along with the research objectives, significance, and questions. The study is focused on developing a workable framework, instead of suggesting new regulation.

With this basis, the next step is to review the existing body of knowledge. Chapter 2 reviews the relevant literature on ERP systems, outsourcing practices, and the regulatory environment of GDPR and Indian privacy laws, which will provide the base for shaping the framework in further chapters.

CHAPTER II: REVIEW OF LITERATURE

This chapter reviews the existing literature relevant to this study. It outlines the theoretical foundations of ERP systems and data privacy, critically examines global and Indian regulatory frameworks such as the GDPR and DPDP Act, and identifies key implementation gaps. It explores key theoretical and regulatory perspectives, identifies legal and operational challenges highlighted in prior studies, and sets the foundation for developing the proposed Privacy Information Management System framework in upcoming chapters.

2.1 Theoretical Concepts

The increasing global focus on digitization has accelerated the adoption of ERP systems across industries. ERP systems, according to Davenport (1998), are integrated software platforms that manage and automate business processes by linking various organizational functions into a unified system. This enables firms to operate efficiently by streamlining operations and maintaining data consistency. Alter (1999) further explains that ERP systems rely on a unified database to confirm that operational data is consistent across functional areas. These systems often include modules that can be customized reliant on the specific needs of an organization, such as sales, distribution, and finance.

However, the implementation of ERP systems, while advantageous, poses significant challenges, particularly in areas connected to data security and privacy. The introduction of the GDPR by the European Union has imposed strict requirements on organizations to protect personal data, including those implemented through ERP systems (Esteves and Pastor, 1999). The global nature of ERP adoption where data frequently crosses borders means that organizations must now comply with GDPR's stringent standards, even if their operations are based in non-EU countries like India (Davidson, 2023). Thus, the critical need for robust privacy frameworks, particularly in countries with developing data protection laws like India, is more pronounced than ever.

ERP systems have evolved from on-premise models to cloud-based solutions, providing organizations with scalability and cost-efficiency (Hadidi *et al.*, 2020). However, as these systems increasingly rely on cloud infrastructures, they are also more vulnerable to privacy breaches and cyberattacks (Lachaud, 2020a). This underscores the need for organizations to develop comprehensive privacy frameworks that are aligned with international standards such as GDPR.

2.2 Growth of ERP Systems and its Implementation

The focus for Enterprise resource planning has started from late 90's for research and development (Davenport, 1998). During the period of 1992 to 1997, Germany's SAP experienced significant growth, with its revenue increasing to approximately $3.3 billion in 1997, making SAP one of the world's fastest-growing software companies. Competitors such as Oracle, Baan, JD Edwards as well as PeopleSoft also observed a surge in demand for their software packages during this period. As a result, Organizations began to see ERP systems as a long-term commitment and a fundamental part of daily operations. One of the key reasons for the emergence of ERP as a software solution was the need to address the challenges associated with managing multiple computer systems, such as high costs for storing and organizing redundant data, re-entering, and converting data across systems, and programming communication links between systems for data transfer. Additionally, Davenport (1998) notes that ERP was designed to address other challenges related to managing business processes, such as improving efficiency and coordination across departments, optimizing resource utilization, technological innovations, and enhancing decision-making capabilities ERP systems were developed in response to the challenges of managing multiple, often redundant, business systems that operated in silos. According to Kumar and J Van Hillegersberg (2000), ERP systems eliminate inefficiencies by providing a centralized platform that manages processes such as finance, inventory, operations and human resources.

Experts describe ERP systems as customizable software packages that integrate information and information-based processes across functional areas within an organization.(Kumar and J Van Hillegersberg, 2000). Typically, an ERP system helps the organization to integrate several functions of various departments like:

1. Finance covering accounts receivable, accounts payable, asset management, cash management, cost management as well as profitability consolidation.
2. Inventory management covering materials forecast and management.
3. Human resources covering payroll management, time management and travel desk.
4. Operations covering sales, marketing, sourcing, life cycle planning, quality assurance and project management.
5. Production maintenance covering equipment management, preventive maintenance scheduling, work order management, spare parts inventory management, and maintenance analytics.

The execution of ERP systems is a complicated procedure that can take a considerable amount of time to complete. Generally, a large corporation will invest hundreds of millions of dollars and several

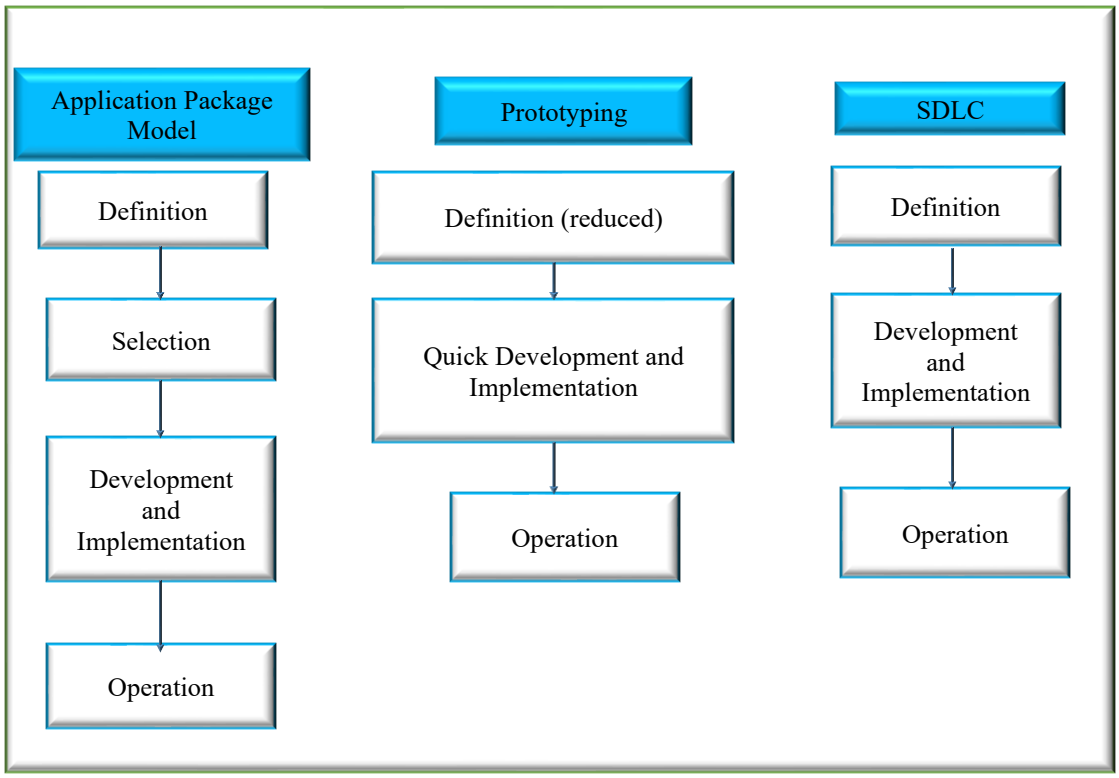
years in the implementation of ERP solutions within their organization. Although implementing an enterprise system quickly can be a wise move for a business, it is crucial to avoid impetuous implementation. Careful planning and execution are necessary to prevent negative consequences for the organization (Davenport, 1998).

To facilitate consistent business operations across various functional areas, Enterprise Resource Planning (ERP) systems leverage an integrated database to support typical business processes (Alter, 1999). Numerous researchers have investigated the challenges associated with implementing ERP systems, with a particular emphasis on developing a framework that encompasses multiple dimensions (Esteves and Pastor, 1999).

In 2000, Van Everdingen and colleagues conducted a survey of over 2000 European companies to investigate the implementation of ERP systems across different industries. Survey results revealed that European midsize companies had a relatively low adoption rate of the major ERP vendors, including JD-Edwards, Peoplesoft, SAP, Oracle as well as Baan. Among the European-based ERP vendors, SAP, and Baan, which are based in Germany and the Netherlands respectively, had a higher level of recognition among European companies compared to the ERP vendors based in the United States.(Van Everdingen, Van Hillegersberg and Waarts, 2000)

Leading software vendors such as Baan, Oracle, Peoplesoft as well as SAP aim to establish a unified database with multiple modules covering the major operations of a company through their ERP systems. IT professionals in the organization should prioritize tasks such as developing business model of the company as well as administering data and databases upon integrating the software package. However, ERP software packages might not be the ideal choice for SMEs because of their expensive price tags, complicated features, and challenging implementation processes. It may be more suitable for these businesses to use combined software packages that cater to local laws and business culture, have limited ERP capabilities, but still assist and integrate common business processes across and within functional areas. Better information is essential for companies to meet the market's demands for faster, higher-quality, and better services and products. However, a full reorganization of the system is often required since the advancement of the organization's information system has lagged the evolution of the business. When this occurs, upgrading the IS and bringing it into alignment with the business system is best accomplished by implementing an ERP system(Ahlin and Zupančič, 2001). An ERP system is an information system that combines aspects of the three traditional approaches to information system development: the application software package approach, the waterfall approach, and the prototyping approach(Ahituv and Neumann, 2002).

Figure 3:Traditional development models



Source: *Author's own work*

While ERP systems provide significant benefits in terms of operational efficiency, they also come with substantial risks, particularly related to data management. The increasing reliance on ERP systems for handling sensitive personal data has led to a growing need for privacy protection measures (Shaul and Tauber, 2013). As organizations shift towards cloud-based ERP systems, the risk of data breaches increases, particularly in environments with weak data protection regulations (Hadidi *et al.*, 2020).

2.2.1 Overview of ERP System Development, Implementation, and Challenges

The system development method is a crucial phase in ERP life cycle procedure as it connects ERP system functions with the organization's business processes, creating touchable operational processes. ERP system can be developed as a software package or developed in-house, and ERP life cycle method is dependent on the system development procedure used. Organizations can choose published system development methodologies such as Microsoft Dynamics Sure Step Methodology, System Development Life Cycle (SDLC), SSM, or create their own framework depending on the type of application package they customize. The proposed ERP system development method is a combination of features from existing methodologies, and the ERP system is built based on two criteria: achieving

the desired objectives of the developed ERP system and saving time and cost during the implementation process (Khaleel and Sulaiman, 2013).

Some of the key characteristics of ERP systems as coined by Chand et al., (2005) are:

- ERP systems are software applications that are readily available and can be integrated into most business processes of an organization company, while still offering some degree of flexibility with customizations,
- ERP systems are significantly larger than traditional business applications in terms of function point measure, business functionality, database size, as well as range of operational and management reports that can be generated,
- ERP systems are highly complex, not only due to their size but also because they utilize common data structures to ensure data availability across different integrated modules rather than passing it from one module to another,
- ERP systems are based on generic business instructions as well as events, and as such, require customization to match the business performance of the organization, often requiring the reengineering of present business procedures,
- ERP systems have a wide organizational reach and require dealing with a large share of the business processes of the organization during implementation and
- ERP systems involve higher costs and are comparatively expensive for implementation without offshore support.

Implementing an ERP system can pose significant challenges in its early stages, such as the need for extensive customization, the decision of whether to handle the implementation in-house or outsource to group companies or external consultants & organization of conflicts of interest among internal as well as external stakeholders. These challenges can transmit over into the post-implementation stage, where decisions must be made about the extent of customization necessary to meet emerging user requirements including data handling and address functionality gaps(Hrischev, 2020a). The Package implementer must also determine whether to rely on group companies or external consultants or build their own in-house expertise, which will affect the costs and practices of maintenance and support, as well as recruitment and retention of internal resources necessary for effective system operation. Failure to address these challenges can negatively impact on usual business operations, potentially foremost to dire significance for the company. (Law, Chen and Wu, 2010)

Package implementation organizations face ongoing demands from various stakeholders, such as customers, shareholders, group companies, global regulations, and suppliers, to enhance their products rapidly and efficiently. To stay competitive in a constantly evolving marketplace and tackle

global challenges, organizations need to be agile with the ability to adapt change in marker needs. (Jha and Pal, 2016)

While the generic stand points for ERP implementations have been summarized above, from Indian context, The number of companies implementing ERP in India is comparatively smaller, and this can be attributed to the high cost and technical expertise required for the implementation process(Saini *et al.*, 2010). However, larger organizations in India are increasingly adopting ERP systems to improve their operational efficiency as well as decision-making capabilities. Major ERP vendors in India include SAP, Oracle, Microsoft, and Tally. Despite the smaller population of ERP implementing companies in India, the trend of ERP adoption is on the rise as businesses understand the advantages of using such systems. (Nandi, Kumar and Pai, 2015) (Nandi and Kumar, 2016) . SMEs face a range of challenges when it comes to implementing ERP systems(Deshmukh, Thampi and Kalamkar, 2015). Effective implementation of an ERP system has the potential to decrease expenses related to operations, data accuracy, and IT maintenance in an organization(Schniederjans and Yadav, 2006), enabling organizations to pursue better strategic initiatives and improve their responsiveness to customers(Bharadwaj, Bharadwaj and Bendoly, 2007).

The key challenges include limited awareness of ERP implementation benefits, perception that it's meant only for large firms, previous implementation failures, customization costs, limited IT resources, low production capacity, ineffective marketing strategies, limited opportunities for modernization and expansion, identifying new markets, dealing with government agencies to resolve issues, trained offshore consultants (Vayyavur, 2015), data management, change management, and capital constraints (A. Deshmukh and Kumar, 2016).

2.2.2 Data Management, Technology, and Security in ERP Systems

Effective ERP implementation requires seamless coordination of data across multiple service touchpoints. This becomes especially challenging in complex information processing scenarios as highlighted by researchers Ramachandran and Voleti (2004) and Jha and Pal (2016). For example, when a user makes a request on a website, multiple service providers may collaborate to fulfill the request. These providers handle specific tasks, and information exchange between them is often necessary to complete a task. For instance, when a user books a trip on an online travel agency, the agency interacts with a hotel, airline & payment provider. Although exchanging information is necessary to complete a task, providers may also collect additional data for personalization purposes, which they could share with each other. However, users may have limited transparency over the information shared with each entity due to the complex nature of these collaborations.(Decroix *et al.*, 2013). Some more practical

implementations include the CRM system, which helps achieve communications with customers. Another example is HRM software, which facilitates employee management. The systems such as MAS, SAR, SCM, and LIS are also types of practical systems that are implemented as a part of ERP packages(Soliman and Karia, 2015).

Accurate data management is crucial for the successful implementation of an ERP system, as incomplete, inconsistent data or inaccurate can negatively impact its performance. Post-implementation data error correction can increase operational costs, reduce effectiveness, and diminish the competitive edge. Therefore, it is vital to identify data quality requirements and take preventive measures. These include planning the data model architecture, analyzing data decisions and responsibilities, converting data from previous systems, and deploying tools to monitor data quality across multiple dimensions, such as accuracy, completeness, and consistency with a formal framework as recommended by Shaul and Tauber (2013).

According to Mehta (2016), successful implementation of ERP in Indian SMEs requires effectively managing issues related to data accuracy, consistency, frequency of use, redundancy, data relevancy, data cleansing, consolidation, transformation, and validation measures to ensure data integrity. This applies both to ERPs implemented from India to group companies and Customer across regions including EU.

Studies highlight that the focus for Recent ERP implementations have shown a shift towards the adoption of Web-based and Cloud-based ERP systems, in addition to the traditional ERP systems. This shift has led to ERP system designers and vendors, such as Oracle, Microsoft, and SAP, focusing on the design of ERP systems based on Cloud technology, which are provided as a service through monthly or annual subscriptions. This service is located outside the organization, eliminating the need for it to exist within the organization.

Cloud-based ERP systems are classified into two types, namely SaaS and PaaS, depending on their infrastructure setup. SaaS provides ready-to-use software and applications that meet the needs of specific business functions and processes. It also enables users to access applications created by the Cloud provider through the web browser interface from different client computers via the Internet(Hadidi *et al.*, 2020).

On the other hand, the traditional ERP system, also known as an On-Premises system, is a type of ERP system provided as a product that needs to be purchased by customers. This type of system requires time for implementation as it requires the installation of hardware and special software in the

customer's location. In this system, the data and application are under the control of the customer, making it a preferred choice for government organizations, especially in EU and MEA countries, which prioritize data security and do not wish to transfer it to third parties.(Hadidi *et al.*, 2020)

Modern ERP systems also develop and implement e-commerce solutions. To succeed in the new e-business landscape, it is essential to incorporate ERP modules such as e-shop, e-orders, e-store, and e-invoice to facilitate business transactions between customers and companies. These modules focus on facilitating business transactions between companies and customers by providing an electronic way to exchange business data or credentials through Electronic Data Interchange (EDI). However, this also sets new necessities for data security as the external exchange of information that requires protection. ERP systems require robust data security measures to protect information regardless of the modules implemented or information exchange. Vendors/Consultants are expected to implement special security methods in the system architecture, data transfer, access, and databases, along with evolving security policies. Important considerations for ERP systems' future include their usefulness to businesses, their compatibility with current technology, and the safety of sensitive info and data (Hrischev, 2020b).

In connection to information and data security, ensuring an adequate level of security is a crucial element in any security strategy as it demonstrates the administration's commitment to security and acquiescence with data safety rules affecting its customers and partners. Insufficient security raises the likelihood of violations, while excessive security can increase IT, software, and hardware expenses, system performance, and business operations. When it comes to ERP systems, there is no one-size-fits-all security solution. Each organization must evaluate risks and establish security objectives that are tailored to its specific environment and the nature of the data it handles. The challenge in performing risk assessments lies in the fact that most risk factor data contain imperfections and uncertainties, such as contradictions, inaccuracies, unreliability, incompleteness, nonlinearity, and dynamic variability of the systems(Kozhukhivskyi and Kozhukhivska, 2022).

2.2.3 Future of ERP Packages and Need for Privacy Framework

In 2022, according to Gartner, Inc., end-user expenditures on corporate application software in India will reach $4.2 billion, up 14.6% from the previous year (Gartner, 2022a).

"*Driven by the digital transformation agenda, Indian enterprises will continue to expand the share of software spending in their broader IT spending. Organizations are increasingly relying on software to operate all aspects of business*," *according to Neha Gupta, VP and analyst at Gartner* (Gartner, 2022a).

Furthermore, Gartner forecasts an increase in ERP investments as more manufacturers push to renovate and replace legacy ERP systems with cloud and hybrid ERP strategies (Gartner, 2022b) Although there is an abundance of literature on ERP implementation in developed countries, particularly in North America and Europe, studies have shown that there is less evidence regarding ERP implementation in developing countries, such as India. (Rupčić, 2021). This situation poses a challenge when compared to Gartner's forecasts on the exponential growth of the Indian ERP business, underscoring the need for a data security framework for ERP implementations from and India.

2.2.4 Summary of ERP application systems Overview

This section summarizes the growth of ERP systems that began in the late 90s, which are essential for managing multiple application systems and improving business processes. Implementing ERP systems is complex & time-consuming, requiring careful planning as well as execution. ERP systems integrate numerous functions across departments, such as inventory management, investment, human resources, operations, and production maintenance to name a few. SME encounter obstacles when implementing ERP systems due to cost constraints, limited resources, and risks associated with data management and information security, which are critical aspects of ERP systems. The adoption of cloud-based and web-based ERP systems is increasingly becoming popular among SMEs. Future trends in ERP implementation include integration with e-commerce platforms and the growing need for privacy frameworks to protect sensitive data.

Table 2:Summary of Key Literature Sources

Authors and Sources	***Themes and Arguments***	***Agreements, Contrasts, and Linkages***
Davenport (1998)	*ERP systems, integration of business processes, and their impact on organizational culture*	*Agrees with Alter (1999) and Esteves and Pastor (1999) on ERP challenges and organizational transformation*
Alter (1999)	*ERP systems, unified databases for business operations across functional areas*	*Agrees with Davenport (1998) and highlights the increasing importance of data consistency across functions*
Esteves and Pastor (1999)	*ERP implementation challenges, complexity, and cost*	*Agrees with Davenport (1998) and Alter (1999) on the significance of addressing ERP challenges*
Kumar and J Van Hillegersberg (2000)	*Customization of ERP systems to integrate functions across diverse industries*	*Supports Esteves and Pastor (1999) on ERP customization challenges*

Van Everdingen, Van Hillegersberg and Waarts (2000)	*ERP adoption in European mid-sized companies*	*Highlights ERP implementation challenges for mid-sized enterprises*

Source : Authour's Own Work

This table summarizes key sources that address the growth of ERP systems and their implications for business processes. The correlations between authors show a growing consensus on the benefits of ERP systems, as well as the challenges posed by their implementation in different regions and industries.

2.3 Outsourcing alliances: India's IT industry expansion

2.3.1 Outsourcing Risks and Considerations for Strategic Alliances in IT Services

According to Elmuti and Kathawala (2001), outsourcing is a strategic alliance, which involves an agreement between two organizations to conduct business in a manner that goes beyond typical business transactions but is less permanent and involved than a joint venture, which involves the pooling of resources to create a separate business entity. A well-planned strategic alliance can provide various benefits, such as enhanced productivity, increased business competitiveness, cross-skilled expertise, accelerated commercial growth, and improved convenience to new markets and unacquainted business domains. The main reasons that impact outsourcing decisions are cost reduction, improvement in strategic operational performance, data security and development competencies(Lambe, Spekman and Hunt, 2002). Although the primary purpose of outsourcing is to reduce costs, it also allows the principal organization to concentrate on its core competencies (Ramachandran and Voleti, 2004).

According to Agrawal et al. (2010), the practice of outsourcing has expanded from its regional origins in the 1960s to encompass the entire globe. This shift can be attributed to the advent of economic liberalisation and globalisation, which have made it possible to outsource products and services beyond national boundaries. Offshore outsourcing, also known as remote implementation, has become feasible due to developments in telecommunication technology and a decrease in the cost of information technology. Accounting, HR payments, ticketing, customer service, application support, package implementation and customer interaction services are some of the outsourced tasks that developing nations like Malaysia, China, India, and the Philippines have traditionally gotten through offshore outsourcing(Kedia and Lahiri, 2007; Agrawal, Goswami and Chatterjee, 2010).

2.3.2 Exploring the Risks and Opportunities of Offshore IT Outsourcing in India

With Y2K issue proving India's competence in IT services, the outsourcing industry in India gained traction following the country's economic liberalisation in 1991. Blue Cross contracted Electronic Data Systems (EDS) to manage its data processing in 1963, marking the beginning of IT outsourcing. Business solutions are provided by EDS, a worldwide IT-enabled service provider. In 1979, American Express began using Tata Consultancy Services (TCS) in India to handle its accounts receivable financial package services, marking the beginning of the offshore outsourcing industry(Anisimova, 2023). Motorola and Texas Instruments both set up shop in India around the middle of the 1980s (Agrawal, Goswami and Chatterjee, 2010). This trend of firms engaged in outsourcing of services beyond national boundaries is termed as tactical outsourcing partnership as coined by Brown and Wilson (2005).

From ERP implementation standpoint, when selecting an ERP vendor, companies may consider factors such as the vendor's location, implementation services, security as well as ongoing maintenance policies. However, total outsourcing can come with a significant cost for obtaining the vendor's services or within the partner organizations. As a result, a lot of businesses consult with vendors or their affiliated organizations; sometimes, internal employees and outside experts work together as a team (Law, Chen and Wu, 2010).

However, many studies focus on examining the factors that contribute to the success of strategic alliances, rather than analyzing reasons for their failure. One of the reasons stated is that offshore IT outsourcing risks are amplified by greater geographical distance and cultural differences between contracting countries, resulting in communication difficulties, misaligned expectations, changes in regulations, and potential data security concerns (Dibbern, Winkler and Heinzl, 2008). Organizations should carefully assess and mitigate these risks before engaging in offshore IT outsourcing (Gartner, 2019).

In order to protect their resources and respond to intrusions and threats, client organizations should conduct due diligence and risk assessments to determine if the service provider has the necessary security measures in place. These measures should include encryption, firewalls, and customer identity authentication (Upadhyay et al., 2010); Hussain et al., 2019).

Establishing an outsourcing partnership is a risky undertaking, as evidenced by numerous reported failures. One of the risks involved is poaching, which is the illegitimate use of a client's critical business data for the service provider's benefit. This betrayal of confidence can hurt the client's company, particularly in offshore outsourcing settings like India, where IP and data security laws aren't always set up properly (Das Aundhe and Mathew, 2009).

Despite the fact that outsourcing's risks need careful examination, Gartner predicts that post 2023, a substantial 65% of larger companies using captive remote or close to shore service delivery centres will have adopted a multi-country sourcing strategy (Gartner, 2019). This makes it increasingly important to study the risks associated with cross-border transfer via outsourcing.

2.3.3 Summary of Outsourcing Risks and considerations for Strategic Alliances in IT Services

This section outlines key milestones in India's outsourcing industry growth due to economic liberalization and globalization, with offshore outsourcing becoming a global trend. However, cross-border scenarios magnify risks like communication difficulties, misaligned expectations, regulatory changes, and data security concerns. Data privacy risks are especially crucial when sharing sensitive business data with service providers/global delivery centers in countries with weaker data protection frameworks, leading to trust breaches. In countries like India, where data security and intellectual property rights frameworks may not be well-established, data poaching risks are heightened. Despite these challenges, larger enterprises are expected to adopt a multi-country sourcing approach for offshore or nearshore service delivery. Therefore, understanding the risks associated with cross-border outsourcing becomes increasingly vital, considering India's role as a data processor.

2.4 Data Privacy and GDPR context

This section begins with an overview of the data privacy landscape, followed by a detailed analysis of GDPR principles. It also evaluates their relevance and application within the context of modern ERP systems.

2.4.1 Privacy Risks and Personal Information Risks, and Implications

It has been hard to define and legalise privacy because of varying interpretations across different cultures, locations and time periods. The first people to say that privacy is "the right to be left alone" were Warren and Brandeis (1890). The idea of information confidentiality, also known as data privacy, emerged in the 1960s with the advent of electronic data processing. Westin later defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." His definition highlights the crucial role of individual control over the sharing of personal information (Laughlin, 1968).

Although definitions of privacy existed in the 1960s, the efforts to safeguard privacy gained momentum in the 2000s. The European Union started to impose limitations on exporting data to

organizations situated in countries without adequate privacy protections, in order to protect individuals' privacy. The absence of such safeguards has led to the mistaken belief that personal information can be used without restraint. For families that prioritize their privacy, ensuring their personal data remains secure may require an annual investment cost of $200 to $300 and a significant amount of time for compliance(Gellman, 2002). Lack of privacy information protection has risks for businesses, consumers, and society as outlined below:

Table 3:Privacy risks for business and consumers

Businesses	***Consumers***
Loss in sales due to Lack of Privacy	*Higher Prices*
One Retailer's Loss is another Retailer's Opportunity	*Junk Mail, Telemarketing, Identity Theft*
Lost International Opportunities	*Internet Effects*
Increased Legal Costs, Investor Losses	*The Dossier Society for privacy records*

Source : (Gellman, 2002)

According to Heckle and Holden (2006), traditional risk assessment approaches do not adequately consider privacy implications of information systems. Additionally, the authors point out that information security risk assessments do not provide sufficient guidance on how to categorize data according to their confidentiality and sensitivity. Therefore, the authors recommend utilizing privacy impact assessments (PIAs) as an effective means of addressing privacy concerns in such imminent systems. Further research by Fritsch and Abie (2008), showcased that consulting and insurance companies have amassed a significant amount of data on various types of information system risks and the resulting damage to businesses. However, the traditional approach of estimating monetary damages by analysing past incidents of similar nature is inadequate. Currently, there is no clear and compelling classification of privacy risks and their associated costs. This highlights two areas that require attention: the absence of empirical evidence on privacy damage to both businesses and users, and the ambiguous concept of damages and costs relating to privacy breaches, particularly concerning the personal information lifecycle. The literature inadequately defines privacy risks, and the use of subpar protection technology can result in the destruction of information-based applications.

To effectively address privacy risks in information system design, a privacy methodology is essential. This methodology should determine the appropriate level of privacy protection required to mitigate risks while ensuring that the necessary investment is reasonable. Additionally, tools that

facilitate process modelling and lifecycle management of personal data are necessary for the efficient construction of privacy-respecting infrastructures (Fritsch and Abie, 2008). These tools can deploy privacy strategies such as firewalls, anti-spyware, and encryption to assistance organizations quickly recognize and mitigate confidentiality risks, reducing the likelihood of privacy breaches and promoting consumer trust(Oomen and Leenes, 2008).

On the contrary, further exploration of the definition of privacy reveals that it is linked to personal values and beliefs, whereas personal information is an impartial representation of a distinct person. Privacy is built upon the foundation of personal information, and it is only viewed as such when it is placed in a specific context and evaluated according to societal norms. The activities of collecting, using, retaining, disclosing, and disposing of personal information involve both individuals and organizations and are collectively known as privacy. Therefore, not all personal information is considered private (Chang, 2010; Johnson, 2011).

“Personal data or Personally identifiable information (PII)” encompasses information that can directly or indirectly identify an individual. This information can include a person's physical, psychological, economic, cultural, or other traits that are indicative of their identity within society(Rana, 2022).

Some of the Personal information referred are presented in table 4 below.

Table 4: Personal Data or Personally identifiable information (PII)

PERSONAL DATA OR PERSONALLY IDENTIFIABLE INFORMATION (PII)		
• Full Name • Home address • Email address • Date of Birth • National ID Numbers • Passport Number • Events Attended • Social Security Numbers • Location Information • Driver's License number • Visa Permit Number • What are you doing when/status • Vehicle registration plate number • Sexual orientation • Gender • Disability information	• Criminal Record • Photos • Grades • Salary • Education History • Place of Birth • Employment History • Job Position • Generic information • Mother maiden name • Insurance details • Medical information • Credit card Number • Air ticket bookings • Places visited	• Work details (company name, address, phone number) • Dependents • Family members details • Bio Metric data – retina, face, fingerprints, handwriting • Email Address • Password • IP Addresses • Digital Identity • Cookies • Social Networking sites usage • Password hashes • Session information • Friends Name • Membership details

Source :(Gonzalez-Granadillo et al., 2021; Impelsys, 2019)

As the information system applications continue to evolve to meet market needs, privacy risks are increasingly prevalent in the digital age. The risk of privacy breaches is greater than it has ever been before due to the massive increase in the collection and sharing of personal data (Saxena, 2021). So, in order to identify privacy risks and find out how to mitigate them at the early stages, businesses must undertake a privacy risk assessment. A PIA is typically performed proactively during the start of design phase of a scheme, and it involves analysing processing activities, assets, inter-dependencies, real-time threats, vulnerabilities, and Personally Identifiable Information (PII) that may occur throughout the system's dynamic life cycle(Gonzalez-Granadillo *et al.*, 2021).

By showing a thorough privacy risk assessment, organizations can identify potential privacy risks and take appropriate actions to protect sensitive information(Abu-Nimeh and Mead, 2010).This can include implementing privacy-focused tools and technologies, training employees on privacy best practices, and establishing clear policies and procedures for data collection, storage, and sharing(Degerman, Eckerbom and Gu, 2019). Ultimately, a robust privacy risk assessment can help organizations build consumer trust and check compliance with applicable privacy laws and regulations(Gonzalez-Granadillo *et al.*, 2021). The key focus in PIA is summarised in the table below:

Table 5: Data Protection Impact Assessment (DPIA) Check points for organizations (bound by GDPR)

Section	Explanation
1. The essential for a DPIA	Project goals, data processing types, and justifications for utilising a DPIA as a controller/processor
2. Data processing	Nature: data gathering, processing, storage, and deletion procedures; data origin; information about data sharing; probability of data processing involving high risk
	Scope: details regarding the data, whether it pertains to specific categories or criminal offences, the frequency and size of data collection, the span of time data is kept, the geographic area covered, and the number of people impacted
	Context: information about children or vulnerable groups, the level of control individuals have over their data, the nature of the relationship among the data controller or processor and the individual, the expectations of individuals regarding the use of their data, the novelty of the data processing, any security issues or public concerns regarding the data processing in the past or present, the technology available for data processing, and whether the controller is a member of any recognised code of conduct
	Purposes: objective of the project, the desired results for people, the advantages of data processing for the controller, and more general advantages
3. Discussion between the controller and interested parties	Information security and other expert consultations, the controller's procedure for consulting with pertinent stakeholders, the project's collaborating partners, the necessity and timing of collecting individuals' opinions on their data, and any other relevant consultations

4. Compliance and proportionality measures	The nature of the data given to persons and methods to support their rights; the legal basis for data processing; alternative methods of accomplishing project goals; measures to guarantee data quality and data minimisation; measures to guarantee that analysts and processors of data follow all procedures as specified; strategies for ensuring the security of data transfers between countries (if any)
5. Consequences of privacy risks	The data privacy risk's origins, the kind of harm it could do to the person, the risk's severity and likelihood at the outset, and the residual status after the response
6. Mitigation	Precautions made to lessen or eradicate potential privacy hazards

Source: (Bondre, Pathare and Naslund, 2021)**.**

The PIA elements in regulation recital 90 of GDPR overlap with ISO 31000:2018's risk management components. Personal data protection should follow the implementation of security measures, including risk assessment. Two types of output data are generated: records of processing activities and control metadata, which can be used for internal audit or regulatory purposes(Mironeanu and Aflori, 2021). Many countries emphasized the position of complying with regulations, laws, and codes of practice but viewed the main purpose of Privacy Impact Assessments (PIAs) as identifying privacy comprises and addressing them comprehensively. PIAs considered all features of privacy, not just data safety. The US, Australia, and UK recognized the scalability of PIAs, while other countries followed a process template approach. In Canada and the US, third-party audits were conducted, and government institutions were required to send the PIA to the Privacy Commissioner (Borking, 2012).

2.4.2 Data Protection Impact Assessments (DPIA) and Their Impact on Privacy and Corporate Affairs

The European Commission proposed the GDPR on January 25, 2012, which mandated DPIAs for data supervisors and processors whose activities posed exact risks to data subjects' freedoms and rights. DPIAs assessed the impact of the processing activities on personal data protection(Abie and Borking, 2012). According to Article 35 of GDPR, if an organization handles Special/Sensitive Data

(defined in Article 9), it is compulsory to conduct a DPIA. The DPIA is aimed at identifying and documenting potential risks to the rights and freedoms of individuals(Harding, 2018). The goal of a PIA is to comportment a systematic privacy risk valuation, including finding organizational and technical privacy threats. It is recommended that these assessments are done early in the development of an IT application to allow for privacy-enhancing techniques and measures to be proactively built into the application, following the principle of "privacy-by-design"(Oetzel and Spiekermann, 2012) .

The risk-based approach in data protection requires that data controllers expand their responsibilities as the risks related to personal data processing increase. They must identify and mitigate potential risks using appropriate measures such as data minimization, access controls, and encryption(Bańka, Soczyński and Wasiak, 2022). Studies have been conducted to assess whether the term PIA has broader implications than "data protection impact assessment" due to the wider scope of privacy beyond personal data processing. For organizations that handle personal data, performing a PIA can be a challenging and confusing undertaking(Abie and Borking, 2012). This is largely because there is a lack of clear instructions on how to conduct such an assessment, and there are numerous methods available to choose from. However, it remains unclear whether DPIAs will be used solely for compliance with European data protection framework's legal requirements(Berendt *et al.*, 2017).

As data protection grew in importance, the Court of Justice of the EU began emphasizing the GDPR as the primary legal obligation to protect personal data at a high level, with no compromise towards this commitment. The GDPR is consistent with the Court's decisions, particularly in cases such as Google v Spain on the "right to be forgotten" and Facebook v Ireland on Safe Harbor(Albrecht, 2016). The EU GDPR defines personal information or personal data as any information that pertains to an identified or identifiable natural person (data subject) (European Commission, 2018). The GDPR applies to all businesses that process personal data of EU citizens, regardless of where the business is located.

Table 6:Evolution of GDPR

Year	**Revolutionary in the Growth of GDPR**
1970s	Data protection discussions and regulations began in Europe.
1981	The Data Protection Convention (Convention 108) was set up by the Council of Europe and was the first data protection regulation.
1995	The European Union adopted the Data Protection Directive (Directive 95/46/EC), harmonizing data protection laws across EU member states.

2009	The Lisbon Treaty, which entered into force, expanded the legal basis for data protection in the EU.
2012	To meet the new problems caused by technology, the European Commission suggested a complete overhaul of data privacy regulations.
2016	The European Union adopted the GDPR to replace the Data Protection Directive. GDPR was scheduled to come into effect in May 2018.
2018	GDPR officially came into effect on May 25, 2018, marking a significant milestone in data protection regulation worldwide.
2018	The GDPR introduced new requirements for data protection, including stringent consent rules, the right to be forgotten, and mandatory data breach notifications.
2020	With the goal of achieving uniformity in GDPR implementation throughout the EU, the EDPB(European Data Protection Board) was formed.
2021	The UK implemented its own version of GDPR, known as the UK GDPR after Brexit.
2024	Ongoing evolution and adaptation of GDPR to address emerging privacy challenges and technological advancements.

Source: (Linden et al., 2020**)**

This table provides a chronological overview of GDPR's evolution, starting from its inception in the 1970s to its implementation in 2018. It highlights the key milestones that have shaped global data protection standards. The establishment of the EDPB in 2020 and the UK's adoption of UK GDPR in 2021 further demonstrate GDPR's far-reaching impact. As technological advancements and new privacy challenges continue to emerge, the regulation remains a cornerstone of data protection, influencing global privacy frameworks, including India's DPDP Act. The ongoing evolution of GDPR underscores the need for continuous policy refinement to balance innovation, regulatory compliance, and the safety of specific confidentiality rights.

From a US perspective, it is worth noting that the CCPA defines personal information as any information that can identify, describe, or be linked, directly or indirectly, to a particular consumer or household. This broad definition includes various types of information such as names, email addresses, IP addresses, biometric data, employment and education history, financial information, and geolocation data. The CCPA applies to businesses that collect personal information from California residents and meet certain other criteria(CCPA, 2018).

The newly established European Data Protection Board is responsible for ensuring that DPAs in the European Union and its single market interpret and enforce the GDPR consistently. The Board's consistency mechanism can be used by a concerned DPA to refer cases where it has doubts about actions taken by the responsible lead authority at the main location of a controller. The competent national court is the venue for individuals to contest Board decisions through the implementation act, while the Court of Justice of the EU is the venue for DPAs (Albrecht, 2016).

Streamlining the acceptance of new technologies like ERP, cloud computing, and the Internet of Things in Europe might be achieved through the GDPR, which gives controllers and processors the chance to explain their roles, duties, and accountability obligations. According to Article 28 of GDPR, controllers may also act as processors (see "is Processor" in the "Controller" class). However, they cannot act as both processor and controller simultaneously(Matulevičius *et al.*, 2020). To comply with the GDPR, processors must consider how they can become more accountable organizations, given their improved legal responsibilities and potential for joint responsibility below the regulation. Although this is one of the secondary objectives of the GDPR, it is a potential positive outcome with growing trend in information systems (Vranaki, 2016).

The GDPR enhances data privacy rights for EU citizens and imposes significant penalties for non-compliance, placing pressure on controllers and processors(Raschke *et al.*, 2018). However, there are still uncertainties regarding the extent to which technology and framework needs to be adjusted to comply with the law(Gupta, 2019).

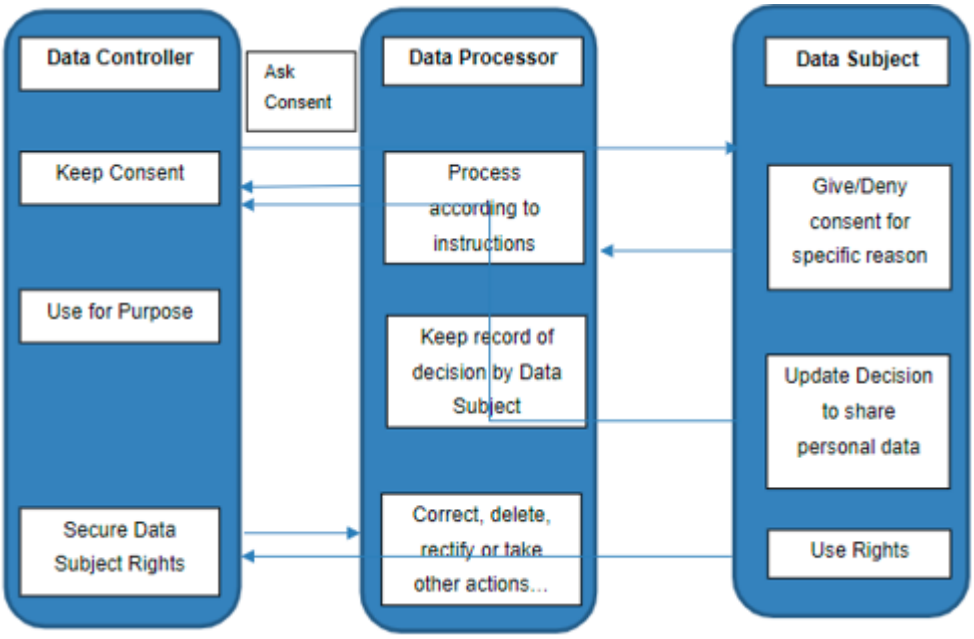
Establishing a proper relationship between data protection and corporate affairs is crucial. The corporate world is impacted by various factors such as accessing, sharing, disclosing, and processing data. The custody of data by the processor or controller plays a vital role in the corporate sector, and private organizations have a responsibility to decide whether to share data or not. This often leads to conflicts between private and public organizations and enforcement agencies. Therefore, it is important to deploy a Privacy framework that combines the different aspects of data protection, including data collection, processing, storage, security, and access, to give data security a specific status as a right(Ghosh and Shankar, 2016).

The GDPR requires processors and sub-processors to demonstrate that they can implement appropriate technical and organizational measures to meet the regulation's requirements and safeguard

data subject rights (Article 28 of GDPR)(Korff and Douwe Korff, 2016). Data processors must ensure data integrity and privacy in compliance with the instructions from the data controller. A written data processing agreement should be in place to detail the nature of their relationship, including data processing duration, type, instructions, and obligations. The data controller is the sole decision-maker and can hire a sub-processor. Both parties must cooperate with the supervisory authority on request(Ashraf, 2021).Privacy-by-Design involves proactively integrating privacy considerations into the design and operation of information systems, technologies, and business practices. This approach requires organizations to identify and eliminate privacy risks throughout the entire data lifecycle. This can be achieved by reconsidering data processes and not processing unnecessary data elements that are not critical for the desired purpose(Karyda, 2018). However, limited research has been conducted on why developers struggle to create privacy-preserving systems while adhering to GDPR principles. Developers' limited knowledge of GDPR principles and a greater emphasis on functional requirements over privacy considerations are significant obstacles to GDPR compliance and Privacy risk management (Alhazmi, Asanka and Arachchilage, 2021). Both controllers and processors, including sub-processors, must demonstrate that they can implement or have implemented suitable security measures appropriate to the privacy risk posed by data processing. (Article 32 of GDPR)(Korff and Douwe Korff, 2016).

When transferring personal data to a third country without adequate protection, Article 46 provides special means for demonstrating appropriate safeguards without requiring specific authorization from a supervisory authority. These special means include legally binding and enforceable instruments such as formal agreements between public bodies in the exporting and importing countries, approved codes of conduct, certification mechanisms with binding and enforceable commitments by the controller or processor in the third country, and standard data transfer clauses adopted by the Commission or a DPA and approved by the Commission. These special means, in and of themselves, provide conclusive evidence of the provision of relevant safeguards for data transfers to third countries without adequate data protection(Korff and Douwe Korff, 2016). In some instances, the economic value of data being transferred across cross borders is not evaluated quantitatively from the perspective of Privacy, national security and legal expectation for which the impact is not clearly analysed in cases where the processor of data does not have a regulation exclusive for privacy(Rieti Ito et al., 2019).

Figure 4:Data Controller Vs Data Processor Vs Data Process flow.



Source: (Ashraf, 2021)

The implementation of the GDPR presents a significant obstacle for companies and their management systems toward framework redefinition. As a result, there has been a surge of activity aimed at analysing the methods of data storage, the systems in place for containing the data, and the implementation of strict control measures. Access policies were developed and implemented, data processing staff are being trained, and reviews of relationships with suppliers and customers were conducted. According to recent Data Breach Investigations Report released by Verizon, Healthcare is the industry that has experienced the majority of data breaches(Verizon, 2020).

Corporate industries, such as package solutions, banking, and healthcare, that primarily deal with individual customers and smaller organizations that process large volumes of personal data, such as online game studios, are feeling the impact of the GDPR. They must account for the processing of email data in their existing systems and databases, a task that can only be automated with a modern customer relationship management (CRM) system. Obtaining consent for data processing has proven to be a significant challenge for these companies, exposing the extent to which their CRM systems can handle it. The GDPR also affects business management systems, which store vast amounts of personal data for users, partners, suppliers, and customers. The efforts are focused on managing stored information, with requests for data from individuals being relatively uncommon(Ali and Miller, 2017). However, these requests are likely to increase over time, leading to the need for new data exchange standards and changes in companies' systems towards approach to comply with GDPR expectations both for data controllers and processors in offshore(Larsson and Lilja, 2019).

2.4.3 GDPR Compliance and ERP Systems

The GDPR introduced a complete framework for protecting personal data, imposing stringent requirements on organizations that process the personal data of EU residents. This regulation has far-reaching implications, particularly for non-EU countries like India, whose software companies frequently serve EU clients. GDPR mandates that organizations adopt measures such as data minimization, clear consent from data focuses, and the appointment of data protection officers (Anwar et al., 2018).

The shift towards cloud-based ERP systems further complicates compliance, as organizations must ensure that data stored in the cloud is adequately protected. ERP systems, which typically handle large volumes of personal data, are particularly vulnerable to data breaches, making compliance with GDPR's stringent requirements all the more critical (Lachaud, 2020).

ERP systems handle large amounts of personal data, making GDPR compliance a major challenge, especially for Indian companies serving EU clients. To meet GDPR requirements, businesses must strengthen data security, conduct regular audits, and follow privacy-by-design principles. Ensuring compliance is key to maintaining trust and long-term business relationships(Arola, 2019).

While GDPR sets strict data protection rules, different countries have their own regulations. India, a major IT outsourcing hub, faces challenges in aligning its data privacy laws with GDPR. The next section compares GDPR with Indian legislation, highlighting key differences and their impact on businesses handling EU data.

2.4.4 GDPR Vs Indian Legislation for Data privacy

When it comes to Offshoring from EU, India has become a leader in IT development and Business Product Management (BPM) services, generating $150 billion in consolidated revenue from 2015 onwards, particularly through offshoring from the EU. This growth is evident as the country's business process management (BPM) sector experienced double-digit growth of over 14 percent in FY22 compared to FY21, with revenues reaching $44 billion. According to a NASSCOM report, the BPM sector in India accounts for nearly 40 percent of global sourcing spend, indicating its significant role in the outsourcing market. This aligns with the fact that many European companies outsource and offshore personal data-related activities to India, highlighting the potential of the European market as a €41 billion market for outsourcing(IANS, 2022). Existing provisions are difficult to understand and interpret because there is no dedicated legislation and no robust regulatory and mechanism for enforcement for safeguarding individual information. India is undergoing significant changes in its economic and information technology sectors. Although it encounters a basic obstacle, the outsourcing sector is a big

help to international investment and economic growth (Wankhede, 2017). The Indian market is open to investment and outsourcing; however, limitations exist due to its weak regulatory framework and inadequate legal safeguards of personal data. There is a lack of conformity with the strict standards set out by the European Union's data protection laws in India, despite the fact that the country is a popular outsourcing location for businesses in the EU (Gupta, 2019).

The IT Act of 2000 and the IT Rules 2011 (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) impose legal obligations on businesses while indirectly protecting personal data(Wankhede, 2017). The IT Act, 2000, the IT Act, 2011, and the rules that are associated with it constitute the bulk of India's data protection legislation. In the event of a data breach from computer systems, the IT Act offers remedies irrespective of the perpetrator's location, provided that the crime is perpetrated on an Indian system. The unauthorised access to, or use of, computer systems or the data stored therein is also addressed in this statute. Moreover, it establishes individual responsibility for the identical. Internet and network service providers, as well as data handling entities, are specifically not encompassed by this section. The main topics covered by the IT act include the following: the legal recognition of electronic signatures and documents; offences and violations; and the mechanism for adjudication for cybercrimes. Agarwal (2020) notes that the act was amended in 2008 to include new crimes such as cyber terrorism and child pornography, as well as new terms like cybercafé, new responsibilities for inspectors and intermediaries, and a stronger focus on data privacy and data security. The act also neutralised digital signature technology. Damages and criminal penalties are provided for under the IT Act in the occasion of a data breach or unauthorised disclosure.

Nevertheless, privacy-related laws are non-existent in India. While India's Supreme Court (SC)has clarified that the right to confidentiality includes safeguarding a variety of information types—including personal, financial, medical, and biometric data—the right to privacy has not been officially defined in the country. Businesses that handle sensitive personal information are subject to civil liability under Section 43A of the IT Act, 2000. This law establishes a system of damages in the event that data security is compromised. According to section 69 of the Act, the government can use computer resources to intercept, monitor, and decrypt information. Any information created, stored, or hosted on any computer resource can be blocked at the direction of any government agency or intermediary by the government or any officers authorised by the government. Data protection guidelines are provided by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

The term "body corporate" has been broadly interpreted to include a variety of business structures, such as sole proprietorships, associations of individuals engaged in commercial or

professional activities, and firms. As an example of a technical standard that fulfils the requirement of "reasonable security practices" (Sukumar, 2017), the regulations mention the ISO/IEC 27001 standards on IT security.

Section 72 and Section 72A of the Indian IT Act outline the punishment for disclosing information obtained through electronic means. Section 72A stipulates that individuals who disclose information obtained in breach of a lawful contract can be punished with a term of imprisonment up to three years or a fine up to five lakh rupees, or both. Section 72, on the other hand, states that anyone who discloses electronic records, books, registers, correspondence, information, documents, or other materials obtained without consent can be punished with a term of imprisonment up to two years or a fine up to Rs 1,00,000, or both, which is approximately equivalent to around 1300 USD or 1200 Euros. (Rao, 2020; Rana, 2022).While the IT Act as well delivers a mechanism for redress in the occurrence of data breaches and complaints, it lacks clarity and independent supervision, more focussed on information security than personal data protection and does not grant specific rights to data themes.

In contrast, the GDPR in the European Union establishes clear data subject rights and requirements for data organizers and processors, as well as an independent supervisory authority. To bring India's personal data protection law in line with the GDPR framework, the government is considering a bill that would provide data subjects the same level of protection whether they are the controller or processor of their data(Chaturvedi and Sinha, 2017) .

Any business or organisation that deals with personal information (including sensitive information) must have a policy in place to protect the data. Rules regarding the categories of data collected, their uses, disclosures, reasonable security practices, procedures, etc., must be comprised in the privacy policy. In order to collect sensitive personal data, the body corporate must first notify the information provider and get their consent. The data will be utilised exclusively for its intended purpose, and the data's original source will be given ample time to review and correct it. Except in cases of legal requirement or an existing agreement, no third party shall be granted access to the data without the data provider's express consent; however, the data under protection is general and not related to privacy (Kolekar, 2015).

In 2017, the supreme court of India recognized the right to object as a fundamental right below the Constitution's right to privacy, similar to GDPR's Article 21. However, India lacks a comprehensive privacy law that covers all aspects on Privacy(Sukumar, 2017). Due to the lack of defined guidelines or principles for the treatment of specific data, regulators encounter challenges when trying to identify data leaks, ensure that third-party apps responsibly use data, and track broad trends in sectors collecting sensitive data (Rana, 2022). Furthermore, there are a number of reasons why the Indian government can't

do more to safeguard private sector data. One of these is that there isn't a specific data protection law, which leaves regulators confused about what counts as a security breach or illegal access by third parties (Wadhwa and Bains, 2022).

In July 2017, the Indian administration recognized the Data Protection Committee (DPC) to investigate concerns connected to data protection in India. The commission was controlled by SC Justice B.N. Srikrishna and was taxed with creating an outline for data safety in India. The board prepared a draft bill on privacy and submitted its report on July 27, 2018, but it has yet to be tabled in the Indian Parliament even after several annexures as of PDP 2021 and recommended the implementation of a comprehensive law on data protection(Burman, 2019). The JPC's report on the DPB 2021 has a crucial role in the growth of India's legal framework for data privacy and protection.

Though the bill has yet to be introduced in Parliament, there has been discussion around proposed changes in the current draft that differ from the previous 2018 and 2019 versions(Rana, 2022). The draft bill had limitations towards the infrastructure availability for securing sensitive data(Sable, 2020), no oversight mechanism for security agencies, obligations for right to be forgotten (Kumar, 2021), economic and implementation challenges of enforcing a law similar to the GDPR in India. As a result, India has not enacted a comprehensive data protection law and is falling behind other countries. Meanwhile, Germany updated its BDSG-Neu in 2017 which existed from 1970, a year ahead of the GDPR deadline in 2018, and has a more developed legal framework on privacy and data protection(Arora, 2020).

From 2018 onwards, both India and Germany made significant changes to their privacy and data security laws. India released a draft Personal Data Protection Bill (PDPB), while Germany revised its existing Bundesdatenschutzgesetz (BDSG) to align with the EU's GDPR. The revised BDSG formed the federal data protection act (BDSG) and state-level acts with each state having their own Data Protection Authority (DPA). In 1970, the German federal state Hessen became the first to enact a law protecting personal data (Arora, 2020). The BDSG didn't come into force until 1978. The GDPR now supersedes the BDSG and realigned to meet the Clause expectations of EU GDPR (Halbach, 2020)

The two countries have different histories in dealing with data protection, with Germany being among the first to implement a regional data protection law in 1970 and India only recently recognizing privacy as a fundamental right in 2017(Arora, 2020).

While both countries address state attention and making a favourable business environment, Germany recognizes the right to privacy in its constitution and has historical experiences with institutionalized privacy violations. India's draft bill follows the format of the GDPR but grants states

additional power with broad exclusions for "safety of state" and legal proceedings, without creating an oversight mechanism for security agencies. Overall, India looks towards Europe and Germany for guidance in emerging its position on confidentiality and data protection(Arora, 2020).

For India to continue to be a competitive outsourcing hub in APAC, it is essential that the country has a strong legal-policy framework in place to protect personal information and data (Singh, 2018). There is a lack of a comprehensive legal-policy structure for data protection and privacy in India, despite the fact that numerous laws, such as the Information Technology Act of 2000, the Indian Contract Act of 1857, the Copyright Act of 1957, the Indian Penal Code of 1860, and the IT Act of 2011 (Reasonable Security Practices and Procedures), do address property rights and privacy partially. Cybercriminals are not deterred by the penalties imposed by current Indian laws, which primarily target state and government-owned businesses (Li, Yu and He, 2019).

Furthermore, the European Commission may leverage the GDPR to bring accusations against non-EU companies, like those in India, of not having sufficient data protection measures, which could delay or even prevent their investments or mergers. Any company that deals with personal information of EU citizens and fails to adhere with the GDPR will face consequences. The growing prominence of offshoring and outsourcing in India highlights the need for a thorough legal-policy framework to safeguard personal information (Chatterjee, 2021).

2.4.5 GDPR Framework Impacts and compliance challenges

In 2018, the European Commission introduced the finalized version of GDPR with the intention of regulating the processing of personal data belonging to individuals in the EU by individuals, companies, or organizations that operate across different regions(European Commission, 2018). The GDPR expands on the types of sensitive personal data that are covered, including data elements that are directly or indirectly linked to a specific person, such as genetic data, location data, and biometric data, mobile identifiers (UDID and IMEI), browser cookies, and IP addresses, MAC addresses, and application user IDs, among others. The regulation places a strong emphasis on transparency and accountability, mandating that organizations get clear agreement from persons earlier processing their personal data and providing them with contact to their information upon request(Comforte cyberedge group, 2020).

The core principles of GDPR (European Commission, 2018; British Standard Institute, 2019) are summarised as:

1. Lawfulness, Fairness & Transparency
2. Purpose Limitation
3. Data Minimization
4. Accuracy
5. Storage Limitation
6. Integrity & Confidentiality
7. Accountability

- EU citizens have the following rights under GDPR (adopted from (European Commission, 2018; British Standard Institute, 2019)):
  - Right of access by the data subject
  - Right to rectification
  - Right to erasure
  - Right to restriction of processing
  - Right to data portability
  - Right to object
- Data processors are obligated to:
  - Appoint a Data Protection Officer
  - Follow data protection by design and default
  - Ensure consent management for all data being collected and processed.
  - Provide appropriate notification in situation of a data break.

According to Capgemini's 2018 report, enhancing consumer trust in privacy and security can boost sales and improve an organization's competitive advantage. GDPR outlines essential privacy and data protection requirements in Article 5, including data anonymization, breach notifications, and secure cross-border data transfer. Research on GDPR's impact on information security is divided into six categories, including user profiling and data collection, business impacts, management and compliance, personal competences, skills and career, authorisation and notification obligation and data storage(Hirvonen, 2022). Organisations that handle personal information of EU residents must reassess their information systems, privacy compliance frameworks, and business procedures to encounter the necessities of the GDPR. Heavy fines—up to 20 million euros of their yearly global revenue—could be levied for noncompliance with the GDPR regulations.

In addition to the possibility of administrative fines for data controllers and processors, the GDPR gives individuals the right to compensation for damages caused by GDPR violations. Articles 8, 11, 25–39, 42, and 43 address certification, certification bodies, processing that does not require proof of identity, general responsibilities of processors and controls, and conditions for children's consent; violations of these articles can result in fines of up to 10 million Euros or 2% of yearly global turnover, whichever is greater. Violators may be fined up to 20 million Euros or 4 percent of their annual global revenue, whichever is greater, for data processing law infractions. These violations can occur with processing, data bound rights, lawful bases for conditions of consent, analysis of certain types of data, or transmission of information to third countries. These articles address these issues (Sing, Matulevičius and Tom, 2018). From 2018 to 2021, fines for non-compliance with GDPR have significantly increased, reaching $332 million by January 2021. Notably, Google was fined $55 million in 2019 for insufficiently disclosing user data collection, while H&M was fined nearly $41 million grusin 2020 for unlawfully keeping excessive records on employees' personal information. These high-profile cases highlight the severe penalties for GDPR violations among large companies. Given that the European IT industry is valued at $155-220 billion USD in Germany and France alone, Indian businesses should prioritize compliance with GDPR to avoid potentially significant impacts (Lekhi, 2021). Despite the severe consequences of non-compliance, there is currently no technical guidance or clear sequential approach available to help organizations evaluate their information systems' business processes for GDPR compliance(Gruschka *et al.*, 2019).

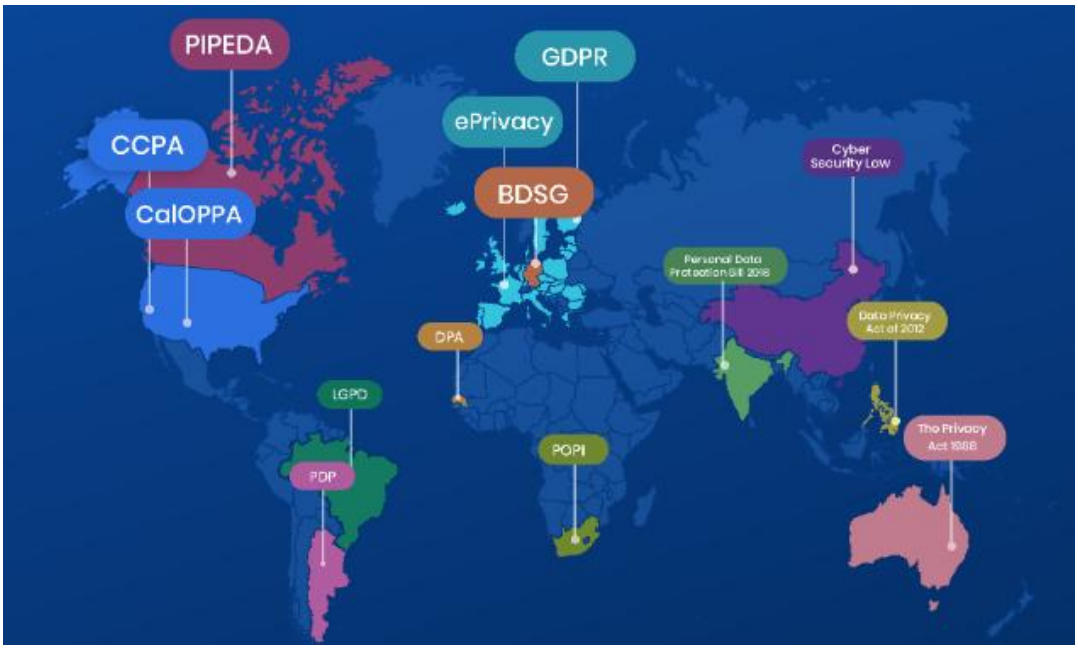
From a Framework definition and compliance standpoint, complying with GDPR is crucial to avoid legal issues and fines. However, a standard framework for GDPR compliance assessment is still missing, making it challenging for organizations with complex systems. GDPR introduces DPIA to identify and address potential privacy issues, but it does not specify which types of processing require DPIA. Proper management of PII is necessary to avoid GDPR violations (Ex:incase of deletion or retention for longer periods), but data controllers must also keep track of personal data associated with data subjects, which can be challenging from implementation standpoint(Bisztray and Gruschka, 2019). To ensure an effective Data Protection Impact Assessment (DPIA), it is essential to take into account the legal, organizational, social, and technical factors.(Dashti and Ranise, 2020).

Organizations seeking information on GDPR compliance for complex systems may face challenges due to the recent implementation of the regulation. While there is extensive information available on ERP implementation through literature and online sources, GDPR research primarily relies on online sources, such as the official EU GDPR website and the Information Commissioner's Office in the UK (Mast, 2018). The GDPR focuses on the personal information of data topics in the EU and the UK, which is following the GDPR even after Brexit(Comforte cyberedge group, 2020). In cases where

GDPR exceptions are applied, such as collecting information for research purposes, additional investigation focused on the legal issues arising from this factor is crucial (Vanezi *et al.*, 2019).

The GDPR grants individuals, rather than businesses or governments, control over their privacy (Comforte cyberedge group, 2020). Although the impact of the GDPR on citizen data and industry practice is open to debate, it is widely recognized that it had a significant influence on national and international governance of data protection and privacy on digital world(Herrle and Hirsh, 2019). This has sparked a global conversation on the subject, with non-EU countries also taking notice(Kuner, 2020). Notably, countries within Europe, including Switzerland, Norway, Iceland, and Liechtenstein, as well as 12+ countries outside the EU, such as California-US, India, Brazil, Australia, Japan, Thailand, Chile, New Zealand, South Africa, China, Canada and South Korea, have updated or introduced their own data protection laws(Aseri, Abdulah and Aseri, 2020). For instance, California's Consumer Privacy Act & Federal privacy law of US, India's proposed PDPB, and South Korea's updates to its Personal Information Protection Act are just a few examples of this trend (Kawintiranon and Liy, 2021)

Figure 5:Privacy regulations around the world



Source : (Bou Chaaya et al., 2021))

GDPR expects Data controllers and processors are allowed to transfer personal data to third countries or international organizations outside EU, only if they have implemented suitable safeguards, and if they ensure that enforceable data subject rights and effective legal remedies are accessible. It is the primary responsibility of data exporters (Controllers) and importers (processors) to evaluate whether the legislation of the destination country enables the data importer to comply with the appropriate

safeguards and criteria covering EU GDPR are satisfied(Czarnocki *et al.*, 2019). However, after a thorough evaluation of relevant Indian legislation, the purposes and conditions for governmental access to personal data are defined as a part of IT act. Even though oversight mechanisms are in place in theory, they are not transparent in practice. While the right to privacy has been recently acknowledged by the Supreme Court of India, the government still enjoys broad exemptions to the data protection regime concerning governmental access to personal data and implementation of IT act(Guaman, Del Alamo and Caiza, 2021).

Fatehi et al., (2020) used bibliometric, scientometric, and visualisation techniques to look at the 155 relevant records in Scopus. These records were then processed for co-occurrence analysis of key terms and concept mapping. In the past two years, mostly in Europe, the number of papers that were published went up sharply. A look at the abstracts of the papers showed that the terms used most often were data protection, privacy, and "big data." There are three main areas of GDPR research:

1) GDPR's general effects,

2) GDPR's effects on information technology, and

3) GDPR's effects on Customer services like finance and health care.

The number of new businesses in India has increased dramatically, and many of these companies have sought to diversify their offerings. The lack of a hierarchical structure makes it difficult to implement the GDPR, and the data they handle does not meet the criteria set out by the law, either because compliance would be too costly or because the company's leadership has changed. Gupta and Joseph (2020) zeroed in on the challenges faced by Indian IT startups in implementing GDPR on their governance, the factors driving their investment in data regulation compliance, the information security standards that underpin GDPR's implementation, and the various aspects of governance that need to be altered by the IT startup. They found that the most pressing issue facing the startup is raising staff awareness of privacy risks and concerns. Additionally, they discovered information security standards that assist the organisation in meeting the requirements of GDPR.

NASSCOM President, R Chandrasekhar, believes that the privacy policy of a country must be in accordance with its cultural and social values. He suggests that legislation related to privacy should be based on the values and social mores of a given country. In a country as vast as India, privacy issues are complex, and it is necessary to elicit views from various stakeholders over a long period. Chandrasekhar emphasizes that a well-structured effort is required to finalize the formulation process and move the

legislation forward. A robust privacy law, tailored to India's reality, will be essential in the coming years and will serve as the foundation of the next digital economy(Saxena, 2021).

Overall, GDPR is a large part of legislation that objectives to protect how personal data is processed and moved inside and outside the EU. But not every Indian business needs to follow GDPR. The GDPR says that Indian businesses must follow its rules if they offer goods or services in the EU, process personal data sent from the EU, or use the personal data of EU residents to make profiles. If an Indian organisation needs to be GDPR compliant, they would need to make sure they have an up-to-date privacy policy, protect the rights of the data subject, figure out if they are a data controller or a data processor, keep records of how they process personal data, make sure it is safe to process personal data, do a data protection impact assessment, and have a privacy policy framework and process for data protection certification mechanism. (Lekhi, 2021b, 2021a).

2.4.6 GDPR Compliance and Certifications

From Compliance and Certification perspective, the endorsement of GDPR certification by EU lawmakers is outlined in Articles 43 and 42, which define the functioning and design of authorization schemes in the data protection outline. While GDPR certification can also develop outside of this regime, particularly to show to the competencies of Data Protection Majors, any third-party body must be accredited according to one of the 21 accreditation procedures planned in Article 43.1 of the GDPR to subject accepted certification under the Article 42/43 regime(Lachaud, 2020).

Prior to GDPR roll out, the ISO/IEC 29100:2011 framework outlines 11 privacy requirements to protect personal information, while ISO/IEC 27018:2019 and ISO/IEC 29151:2017 provide guidelines for protecting personal information in public clouds and personally identifiable information as a part of ISO 27001:2013 annexures(Bou Chaaya et al. 2021). Standards for such as ISO 31000, ISO/IEC 27005, and ISO/IEC 29134, require a risk evaluation to select protective measures. Compliance, known as accountability, is also essential to these standards and is enforced by adhering to accepted information protection principles, including ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 29151.

The GDPR encourages data controllers to implement protective measures that correspond to the level of risk in their data processing activities. In case of system failure, data controllers should have secure backup procedures in place for services, systems, applications, and configurations. This is one of the fundamental principles of privacy established by the ISO/IEC 29100 standard(Bańka, Soczyński and Wasiak, 2022). Certification under the GDPR after its implementation includes more elements than those outlined in the original definition, and the extent to which it conforms to those components is context dependent. Certifications should mainly be definite as an ex-ante implementation handle rather than a

third-party attestation of obedience issued subsequent an effective showing of compliance, according to the monitoring procedure for the code of behaviour set in Article 41 of the GDPR (Lachaud, 2020c). As a start-up for GDPR implementation, BS 10012 +A1:2019 was rolled out, which has a direct mapping of the clauses of the EU GDPR(British Standard Institute, 2018). ISO 27001 supports GDPR compliance by identifying risks and vulnerabilities through frequent audits from information security standpoint(Gupta and Joseph, 2020) and an exclusive control in Annex A18.14. towards Personal information(International Organization for Standardization, 2013).

Later to formalise the British standards, The ISO/IEC based 27701:2019 was rolled out as an extension to Information security standards of ISO/IEC 27001:2013. This is based on extension of Control specific to Personal data (A.18.1.4 of ISMS) to form exclusive standard of ISO/IEC 27701:2019 Privacy information system standards which demonstrates compliance with GDPR and region-specific Privacy requirements(Bou Chaaya et al., 2021). ISO/IEC 27701:2019 offers a framework that helps organizations establish and maintain compliance with confidentiality and data protection regulations across different regulatory environments. This framework enables organizations to execute measures to protect private information along with adherence to regional rules(Javeria Anwar and Qumer Gill, 2020). In a press release, the French Data Protection Authority (CNIL) highlighted the importance of the ISO/IEC 27701:2019 standard in ensuring the safety of PII. The CNIL emphasized that the ISO/IEC 27701 standard is recognized globally, specifies measures for processing personal data and can be a startup for focus on Privacy framework for Non-EU Processors(CNIL, 2020).

Any organisation, no matter its size, industry, or jurisdiction, can benefit from the groundbreaking standard ISO/IEC 27701:2019, which guarantees effective protection and management of personal information. Companies should find it easier to comply with GDPR due to this standard's interoperable design. To fulfil global compliance requirements, it is not yet known if ISO/IEC 27701:2019, GDPR, or both must be implemented. It is believed that ISO/IEC 27701:2019, with its new privacy extension, will develop the GDPR certification standard, assisting trades in creating more effective systems to attain validation, GDPR compliance, and increased marketing value.

The Privacy Information Management System (PIMS) is an ISMS that is committed entirely to protecting privacy, as stated by ISO (ISO/IEC 27701:2019). Despite the May 2018 implementation of the EU's GDPR, no certification standard has been developed to ensure compliance. To facilitate compliance with the GDPR, ISO/IEC 27701:2019 was introduced in August 2019 to formalise BS10012+A1:2019, which are British standards. Unfortunately, there isn't a tonne of information on how ISO/IEC 27701:2019 can help with GDPR compliance in general, since the standard is still in its early implementation stages. When it comes to handling and preserving PII, ISO/IEC 27701:2019

advocates for a thorough risk-based strategy that can help find and lessen the risks (Javeria Anwar and Qumer Gill, 2020).

On the contrary, Lachaud (2020) highlights that the ISO/IEC 27701:2019-based certification could potentially cause confusion and threaten Article 42/43 implementation, but it also provides an opportunity to spread data protection principles beyond EU borders and clarify the relationships between Article 42/43 certification and ISO standards-based certification. The GDPR defines the nature, scope, process, and legal value of certification under Article 42, and the certification is renewable under the same conditions and process as the initial application. If a certified entity fails to meet the requirements for issuance or maintenance, the appropriate managerial authority has the control to remove certification or refuse to renew documentation at the certification body's discretion (Lachaud, 2020a).

Datasets that are structured in IT assets are the primary emphasis of ISO/IEC 27001:2013 and ISO/IEC 27701:2019, whereas the GDPR is applicable to both types of datasets. Data processing and storage on physical supports are also encompassed under the GDPR, which seeks to mitigate potential threats to individuals' rights and freedoms (Anwar, Gill and Beydoun, 2018). While compliance with the standards is not necessary for certification, certification based on ISO/IEC 27701:2019 gives data processors a reliable signal to reassure their clients and makes accountability requirements easier to comply with. In contrast to the GDPR's infrequent use of risk-based approaches to handle more systemic threats to data subjects' rights and freedoms, the ISO advocates for a comprehensive risk-based approach. The implementation of GDPR compliance for non-EU processors, such as India, and the development of the still-untapped DPC market could be facilitated by the adoption of ISO/IEC 27701:2019-based certification (Lachaud, 2020a).

2.5 GDPR vs Indian Legislation for Data Privacy

In this section, we examine how India’s current legislative framework for data privacy compares with the EU’s GDPR. My analysis indicates that while the GDPR provides a comprehensive, enforceable model for personal data protection, India’s approach remains fragmented and security-oriented rather than rights-driven. This lack of integration weakens accountability and complicates compliance for organizations operating across borders.

The GDPR establishes clear rights for data subjects and corresponding obligations for data controllers and processors, supported by consistent enforcement through independent supervisory authorities. In contrast, India’s data-protection measures are still dispersed under various instruments such as the Information Technology Act 2000, the 2011 Rules on “Reasonable Security Practices and Sensitive Personal Data or Information,” and other sectoral regulations. Prior research analyses

(Wankhede, 2017; IANS, 2022) supports this interpretation, emphasizing that India's existing laws do not clearly define personal data rights or establish an independent supervisory authority. This absence of a unified framework creates compliance uncertainty for organizations working across EU–India data exchanges and may weaken confidence among global clients.

This divergence creates practical challenges for Indian IT and BPM service providers that process EU citizens' data. Without a cohesive statutory backbone, firms must rely on contractual assurances and client-specific compliance models to meet international expectations. Overall, the comparison underscores that India's privacy governance still functions as a compliance-oriented system rather than a principles-based rights regime. Bridging this gap through a unified legal framework is critical to strengthen trust, enable smoother EU–India data exchange, and ensure long-term competitiveness in global markets, especially as cross-border data flows become integral to business continuity across EU–India borders.

2.5.1 The Role of the IT Act in India

India's data-privacy landscape has evolved under strong global influences, particularly the EU's GDPR, which has become the benchmark for modern data-protection reforms. While many researchers, including Abdulah and Aseri (2020), note the worldwide convergence toward GDPR principles, my analysis shows that India's current approach still lacks the enforcement depth and individual-rights clarity of the EU framework. This subsection examines how the Information Technology (IT) Act 2000 and its 2011 Rules attempt to address data privacy and why these measures remain insufficient to meet GDPR standards.

The IT Act and the accompanying Rules introduced India's first legal recognition of digital data and security practices. However, they were designed mainly to regulate electronic transactions and combat cybercrime rather than to build a comprehensive, rights-based privacy framework. Although the IT Act and its rules provide some remedies for breaches, they do not cover the full scope of personal data protection in a comprehensive way. Agarwal, 2020) also observes that the act lacks key GDPR principles such as purpose limitation, data minimization, and the right to erasure, while Sukumar (2017) highlights the absence of an independent regulator to enforce compliance or investigate breaches. Consequently, Indian organizations processing EU citizens' data rely on contractual clauses and client-specific standards, leading to inconsistent protection levels and increased compliance costs. For companies in India working with EU clients, these gaps create practical problems and raise questions about trust when handling data across borders.

In practice, the IT Act serves as a procedural foundation but not a substitute for a dedicated data-protection law. To align with GDPR expectations and strengthen trust in cross-border processing, India requires a unified statute—such as the proposed Digital Personal Data Protection (DPDP) Act—that clearly defines individual rights, assigns controller and processor responsibilities, and establishes independent oversight mechanisms. The purpose of this comparison is not only to show the influence of the GDPR on global reforms, but also to highlight why India needs a more unified, rights-based privacy law. Bridging this gap is essential if Indian service providers are to remain competitive and credible in global markets.

2.5.2 Comparative Analysis with GDPR: Impacts on Global Data Protection and Indian Legislation

Building on this comparison, this section examines how the EU's GDPR has influenced data-protection reforms beyond Europe, including India's evolving legal framework. The regulation has become the global benchmark for privacy governance, prompting many countries to revise their laws. Although India has drawn inspiration from these principles, its progress remains uneven. While the GDPR guarantees clear rights for individuals, strict obligations for controllers and processors, and independent supervisory oversight, India's laws still lack comparable clarity and enforceability (Chaturvedi & Sinha, 2017; Aseri & Abdullah, 2020).

Several research studies point out a range of implications emerging from this gap. Chatterjee (2021) warns that non-EU companies, including those in India, risk being seen as having weak safeguards under GDPR, which could discourage investment and limit cross-border mergers. Others, such as Guaman, Del Alamo and Caiza (2021)add that although the IT Act defines conditions for government access to data, its oversight mechanisms lack transparency, allowing the state broad exemptions. Similarly, Sable (2020) highlights shortcomings in India's draft PDPB, particularly weak infrastructure and limited accountability for security agencies. Burman (2019) adds that the proposed Data Protection Committee framework remains stalled in Parliament, prolonging regulatory uncertainty and leaving India without a unified privacy law. Gupta and Joseph (2020) further highlight the practical difficulties faced by Indian IT start-ups in implementing GDPR, particularly the need to strengthen employee awareness of privacy risks.

In summary, these studies show that while India has acknowledged the importance of privacy most notably through the Supreme Court's recognition of the right to privacy - the country has yet to translate this recognition into a comprehensive and enforceable framework. This continuing gap underscores the need for India to move towards a unified, rights-based privacy regime if it is to align with global standards and sustain trust with international partners. For a comprehensive overview of the

evolution of data privacy regulation in India, please refer to Table 7 below, which provides insights into the chronological progression of data privacy regulations in the country.

Table 7:Evolution of Data Privacy in India

Year	Milestone in Data Privacy Regulation
2000	Information Technology Act, 2000 (ITA-2000) introduced basic provisions for data protection.
2008	Amendment to ITA-2000 introduced penalties for data breaches and unlicensed access to computer systems.
2011	Extensive data protection standards were laid forth in the Information Technology Rules, 2011 act. (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)
2017	The right to privacy was proclaimed a basic right within the Indian Constitution by the SC of India.
2017	In order to create a thorough privacy legislation for India, the Srikrishna Committee was established.
2018	Srikrishna Committee released the PDPB, which later evolved into the DPB, 2019.
2019	DPB, 2019 was presented in Parliament, setting the step for comprehensive data protection legislation.
2019	European Union's General Data Protection Regulation (EU-GDPR) came into effect, influencing global data protection standards.
2019	India released the Draft DPB, 2019 for public consultation, drawing from GDPR principles.
2020	The Joint Parliamentary Committee started reviewing the Data Protection Bill, 2019.
2021	The Data Protection Authority of India (DPAI) was proposed as an self-governing supervisory body for information safety.
2022	The Data Protection Bill, 2022, incorporating changes based on public feedback, was introduced in Parliament.
2023	The DPB (DPDP 2023) has been passed in Indian Parliament during August 2023, currently exploring the feasibility of implementation as a legislation which may become permanent law, founding a complete data protection framework in India.

Source: (Gupta, 2019)

2.5.3 Privacy Risks and Data Breaches

While the previous section highlighted the gaps in India's legal framework compared with the GDPR, it is equally important to examine how these shortcomings play out in practice especially in the context of ERP systems, where data privacy risks are most visible. The increasing reliance on ERP systems for managing business operations has amplified the risk of data breaches, especially when these systems are implemented in cloud environments (Davidson, 2023). Privacy breaches can have severe consequences for both businesses and consumers: companies may face significant financial penalties, while individuals risk losing sensitive personal information.

2.5.4 Privacy Breaches Cases

Given the risks highlighted, it is important to look more closely at actual privacy breaches and how weaknesses in systems can reveal sensitive personal information Data breaches are privacy-intrusive events that have a potential to expose sensitive personal information such as sexual orientation, passwords, financials, physical address, and political opinions, and can be caused by cyberattacks or negligence by data holders. These breaches can lead to individuality theft, monetary and reputational harm, and unauthorized use of user accounts. Data breaches can leak private information of millions of data subjects including email addresses, geographic locations, IP addresses, SSNs, genders, names, and passwords.

Three main types of data breaches are organizations' data leaks, collection lists, and spam lists. (Falivene and Falivene, 2021). As we enter the era of Datafication, privacy breaches and lack of control over data pose a significant challenge for antitrust regulators globally. Companies are using data to infer consumer behaviour without their consent, at a lower cost. In this regard, India should consider revising its Competition Law, similar to the German law that recognizes the importance of controlling consumer data and the factors that determine market dominance(Dutta, 2021).

From information applications standpoint, Identifying, analysing, and detecting conflicts in software requirements, especially those related to critical classes like Privacy and Security, are essential strategic activities that help prevent system failures and reduce reengineering costs. Difficulties with data protection regulations like GDPR is crucial as organizations can face significant fines for non-compliance. To comply with GDPR, privacy-by-design activities must be enforced from the outset of the software engineering cycle. As a result, requirements engineers require systematic methods and tools to identify, detect, and resolve privacy and security requirements conflicts(Alkubaisy *et al.*, 2022).

The growing number of Internet users has led to an increase in data, which in turn has resulted in data breaches and theft. However, misuse of user data by data collectors is also a major concern, and data protection laws are in place to prevent such actions. Without adequate or absent data protection laws, preventing data collectors from misusing user data can be challenging. However, in India, there is no legislation governing privacy and data protection, making it difficult to prevent unintentional use of user data by product or service companies(Yadav and Yadav, 2021). These examples of privacy breaches show why strong laws are essential. The next section reviews at how India's DPDP Act compares with the GDPR, and where gaps still exist.

2.5.5 Challenges in India's Data Protection Framework

India's rapidly growing IT sector has made it a global leader in software outsourcing, particularly in the field of ERP implementation. However, India's data protection framework remains relatively underdeveloped compared to GDPR (Saxena, 2021). The release of the DPDP Act in 2023 marks a important advancement in strengthening data privacy regulations. While the act brings India closer to international norms, key gaps persist, particularly in:

- **Enforcement mechanisms** : which lack the stringent oversight and penalties seen under GDPR.
- **Alignment with global standards** : as certain GDPR principles—such as the right to data portability and strict cross-border data transfer controls—are not fully integrated.
- **Regulatory independence** : as India's framework grants significant authority to the government rather than an independent supervisory body, which woud raise concerns on impartial enforcement.

To ensure robust data protection and international business continuity, India must further refine its regulatory approach, bridging the gap between DPDP and GDPR through stronger enforcement, compliance mechanisms, and cross-border cooperation(Sen, 2021). Even with the DPDP Act, weak enforcement and gaps with global standards exist as of date. These problems become clearer when we look at privacy breaches in India.

2.5.6 Privacy Breaches and India's Context

Privacy breaches loom as significant threats, capable of wreaking havoc, including potential identity theft and significant financial losses. Mitigating conflicts in privacy and security requirements becomes indispensable. India's current data protection framework lacks robust legislation, rendering the curbing of user data misuse by product or service companies an intricate challenge (Falivene and Falivene, 2021).

Given these challenges, India must take proactive steps toward strengthening its data protection framework. The absence of a comprehensive legal structure not only increases privacy risks but also

affects the country's global standing in IT outsourcing(Kurt Wimmer, Maldoff and Lee Covington, 2020). The following section explores potential pathways for India to enhance its data protection and privacy regulations moving forward.

2.5.7 The Way Forward for India

H. P. Singh stresses the importance of India having a robust data protection and privacy legal-policy framework to maintain its competitive position as an outsourcing hub. The author notes the coverage of privacy and property rights by various Indian laws but emphasizes the lack of a comprehensive framework for data protection and privacy (Singh, 2018). As India faces challenges in enacting a comprehensive data protection law, it looks towards Europe and Germany for guidance, with the two countries having made significant changes to their privacy and data protection laws since 2018 (Arora, 2020). Singh (2018)underscores the imperative for India, recognized as a prominent outsourcing hub, to establish a robust data protection and privacy legal-policy framework. Ghosh and Shankar (2016) argue that existing Indian laws and penalties are insufficient to deter cyber-criminals, with limitations mostly applying to state and state-owned enterprises.

NASSCOM President, R Chandrasekhar, believes that the privacy policy of a country must be in accordance with its cultural and social values. He suggests that legislation related to privacy should be based on the values and social mores of a given country. In a country as vast as India, privacy issues are complex, and it is necessary to elicit views from various stakeholders over a long period. Chandrasekhar emphasizes that a well-structured effort is required to finalize the formulation process and move the legislation forward. A robust privacy law, tailored to India's reality, will be essential in the coming years and will serve as the foundation of the next digital economy(Saxena, 2021). Furthermore, for Indian startups and SMEs, which are crucial to the economy, a clear and effective data protection framework will be vital in fostering innovation and ensuring compliance with international standards.

2.5.8 India's New Digital Personal Data Protection Framework and Current State of Data Protection in India

In recent years, policy makers, civil society groups, technology experts, and industry bodies have repeatedly emphasised the need for a clear and comprehensive data protection framework in India. These calls gained momentum after the Supreme Court's Puttaswamy judgment in 2017, which recognised privacy as a fundamental right and highlighted gaps in the country's existing data governance structures.

However, progress towards such definition of a framework has been slow. The withdrawal of the Personal Data Protection Bill (PDPB), 2019 during the COVID-19 pandemic illustrated the practical and

political challenges in pushing forward large-scale privacy legislation (Yasir and Singh, 2022). The introduction of the Digital Personal Data Protection (DPDP) Act, 2023 marks an important step in reviving India's data protection efforts. The Act strengthens individual control over personal data by setting clearer rules around consent, purpose limitation, and user rights (DR. Reeta, 2023).

At the same time, the Act has attracted public debate and criticism, largely because of the broad exemptions given to the central government. Concerns have been raised about the potential impact of these exemptions on press freedom, access to information, and the balance between state authority and individual privacy. Critics argue that these loopholes could reduce transparency and weaken the safeguards intended to protect citizens' data. According to Singh Rahul (2023) , although the Act imposes stronger responsibilities on data fiduciaries and outlines explicit rights for individuals, organizations still face practical challenges in adopting it. Many of the operational details such as rules, timelines, and compliance mechanisms etc., remain pending, making implementation difficult for both public and private entities.

The delayed enforcement of the Act reflects a broader challenge: translating legislative intent into effective, real-world practice within a rapidly evolving digital environment. As Cynthia J. Rich, 2023) observes, India must continue to develop a privacy framework that not only protects citizens' rights but also builds public trust and supports cross-border data flows. Strengthening this foundation is essential for India to align with global standards and enhance its credibility in international business and technology ecosystems. In this context, it becomes important to assess the current state of data safety in India, particularly in light of the legislative shifts and emerging regulatory expectations.

2.5.9 Current state of data safety in India

In August 2022, the Indian government removed the proposed PDPB, 2019, which had been under development for more than two years, due to the pandemic. This bill aimed to simplify the process for persons to request the erasure of their personal information and require internet companies such as Google and Meta to obtain permission before using most of a person's data(Al Jazeera, 2022). However, the Government later proposed to create a new law that would align with existing legal compliance frameworks like the EU GDPR and Privacy Shield to enhance data security and privacy in an Indian context. Around the world, countries are taking similar steps to establish compliance frameworks, such as the GDPR in Europe(Singh, 2022). (Yasir and Singh, 2022)

To succeed the defunct PDPB of 2019, the Ministry of Electronics and Information Technology (MeitY) released a new draft bill on November 18, 2022, called the DPDP Bill, 2022. The draft

legislation addresses Data principals' rights and duties, data fiduciaries' obligations and responsibilities, and processing regulations. It also includes the establishment of a Data Protection Board as part of a compliance framework. However, the DPDP Bill is still in the early stages of development and has a long way to go before it becomes a sustained framework comparable to the EU GDPR(Al Jazeera, 2022; Shekhar and Choudhary, 2022).

2.6 Summary of data privacy and GDPR context

The research analysis for this section covered various aspects of privacy, data protection, and the GDPR in the European Union (EU). It began by exploring the evolving concept of privacy, the implications of privacy risks on businesses and consumers, and the importance of privacy impact assessments (PIAs) for addressing privacy concerns in information systems.

The focus then shifted to DPIAs mandated by the GDPR, emphasizing the need for data organizers and workstations to assess the impact of analysing activities on personal data protection, especially when handling sensitive data. Challenges related to conducting DPIAs and ensuring compliance with GDPR were also discussed.

The review further compared data security and privacy regulations in India and the EU, highlighting India's need for a comprehensive privacy law to maintain its competitive position as an outsourcing hub. The GDPR's impact on businesses worldwide, including Indian companies processing EU residents' data, was emphasized.

GDPR's compliance challenges and certifications were also explored, with discussions on the adoption of ISO/IEC 27701:2019 as a normal for GDPR compliance and its potential impact on Article 42/43 certification. Data breaches can have devastating effects, and the review's coverage of privacy breach cases highlights this. To avoid these kinds of problems, software engineers should adhere to privacy-by-design principles.

The review ended with an update on India's data protection landscape, noting the withdrawal of the proposed PDPB of 2019 due to the pandemic and the subsequent proposal of a new Digital PDPB. This bill aims to regulate the processing of personal data and align with existing compliance frameworks like the EU GDPR and Privacy Shield, though it is still in the early stages of Implementation review.

Overall, this sections from GDPR context and Data privacy highlighted the significance of data safety and privacy rules, particularly the GDPR, and the challenges and implications for businesses and individuals in both the EU and India. It stressed the essential for comprehensive legal-policy frameworks

to protection personal data and encourage responsible data handling performs in the digital world for Indian data processors.

2.7 Summary of Literature Review

ERP systems, outsourcing agreements, and data protection are examined in the context of India's ever-changing regulatory environment. The EU-GDPR's pros and cons for India's ERP industry are examined. According to Davenport, Kumar & Van Hillegersberg, and Khaleel & Sulaiman, ERP systems improve company processes, especially for bigger organisations. However, they emphasise SMEs' ongoing issues including information and finance shortages. ERP systems integrate more company operations than ever, making strong security frameworks necessary. Cloud-based ERP adoption has benefits, but customisation, maintenance, and data security are major issues. ERP implementations need greater privacy controls to solve these issues. After understanding ERP dynamics, we may discuss privacy assurance frameworks. This will illuminate the complex relationship between efficiency, regulatory compliance, and technology adoption.

India leads IT outsourcing due to the fast proliferation of offshore service centres since its economy was liberalised in 1991. Outsourcing still saves money, boosts performance, and provides professional knowledge. Outsourcing is raising legal, cybersecurity, and compliance issues for organisations handling sensitive data internationally. Data breaches and regulatory loopholes are major problems, underlining the need for comprehensive privacy rules to secure sensitive data. Due to severe worldwide legislation like the EU GDPR, data privacy is vital. Unlike GDPR, India's regulatory system is continually developing and includes the IT Act (2000), IT Rules (2011), and the planned Digital Personal Data Protection (DPDP) Act (2023). These policies address privacy problems but fail in enforcement, consumer rights, and cross-border data governance. According to the literature, connecting India's data security rules with global principles can improve data security and firm reputation. One idea is GDPR-compliant certification frameworks (ISO/IEC 27701:2019).

Data protection rules in India are poorly enforced, threatening privacy. Unlike GDPR's stringent fines and independent regulatory supervision, India's framework allows state agencies broad exemptions, raising concerns about data exploitation and accountability. Compliance difficulties make meeting global privacy laws difficult for IT and outsourced companies. In light of global outsourcing, privacy-by-design rules, tougher enforcement, and more transparent legislation are needed to safeguard firms and customers. In the context of India’s evolving data protection environment, Enterprise Resource Planning (ERP) systems play a pivotal role in securing corporate workflows. These adaptable software suites improve cross-functional efficiency but demand significant customization and investment. As

hybrid and cloud-based ERP models grow more common, challenges such as high costs, lack of awareness, and stringent data requirements restrict adoption, especially among SMEs. Addressing these concerns requires a dedicated data security framework that ensures both operational agility and personal data privacy.

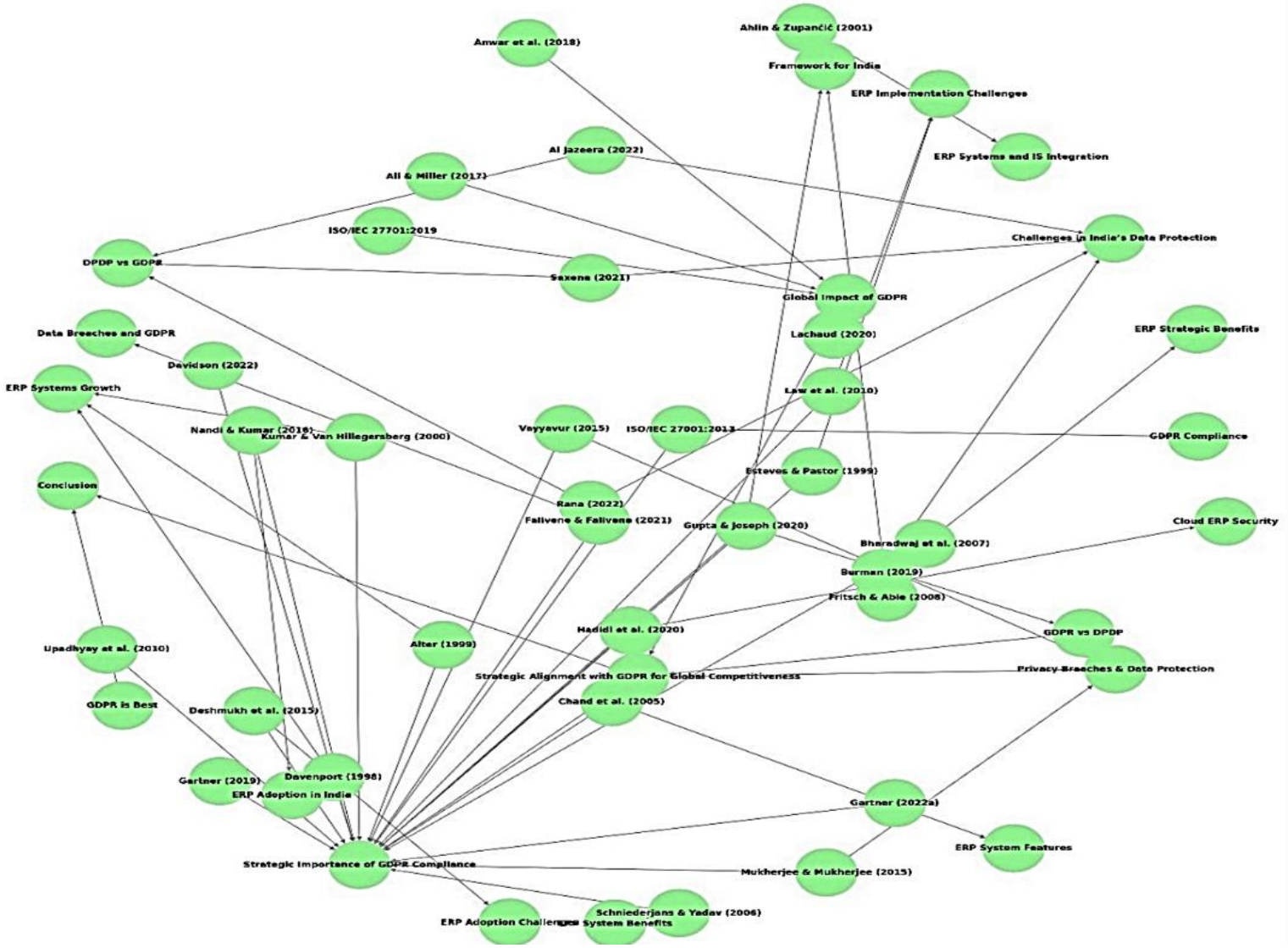
2.8 Interpretation

Based on the overall summary, this literature review provides a comprehensive overview of three important areas in the field of IT in the context of India. Firstly, the review discusses the execution of ERP systems, their benefits and challenges, and the trends towards cloud-based and hybrid ERP strategies in India. Secondly, the review examines outsourcing alliances in the Indian IT industry, including the reasons for outsourcing, the risks involved, and the increasing use of multi-country sourcing approaches. Finally, the review critically examines data privacy norms and GDPR impacts in India, including the requirements for data processors and sub-processors, the state of PDP laws in India like IT Act 2000, IT Act 2011 and the proposed PDPB, and the various Compliance frameworks available to ensure compliance with GDPR.

Overall, the literature review highlights the importance of technology in driving organizational efficiencies and competitiveness in India, as well as the essential for robust agendas to ensure data privacy and security in the Indian context which scarce. The review also emphasizes the challenges associated with implementing technology solutions in India, including customization costs, communication difficulties, and potential data security concerns specific to the Indian environment. With the help of the concisely cited literature references and comprehensive review, it is clear that the efforts of Indian software package organizations to comply with GDPR as a data processor, as well as their relationships with Europe based (like Germany and France) (EU) software package companies, have received very little attention. There is a void in the literature where the responsibilities and roles of Data Controllers and Data Processors from Indian context, along with their respective KPIs, are to be noticed, despite the fact that previous research have advanced the concepts of data Privacy and data Security Management.

The following literature map (Figure 6) provides a visual representation of the relationships between various studies and the themes they explore, such as ERP systems, GDPR compliance, and data protection frameworks in India. The map highlights how studies like Davenport (1998) and Alter (1999) laid the groundwork for understanding ERP systems, while more recent studies such as Davidson (2023) and Saxena (2021) focus on the implications of GDPR for ERP systems and India’s evolving data privacy landscape.

Figure 6:Literature Map showing strategic relationship between ERP systems, outsourcing, Need for GDPR Compliance and challenges in India's data protection



Source: Author's own work

The integration of ERP systems, outsourcing strategies, and evolving data privacy regulations forms a critical foundation for India's digital economy. While ERP adoption and IT outsourcing offer significant economic advantages, they also introduce complex regulatory and security challenges that demand comprehensive governance mechanisms. The global shift towards strict data protection laws necessitates that India strengthens its privacy regulations to align with international compliance frameworks. The literature highlights the importance of high enforcement measures, improved data governance policies, and greater awareness among businesses to enhance digital security and regulatory adherence.

Going forward, future research should explore how India can bridge the gap between existing data privacy frameworks and global standards, ensuring that businesses operating in the ERP and IT outsourcing industries remain competitive while maintaining robust data security and compliance

practices. By proactively addressing regulatory gaps and integrating privacy-centric solutions, India can position itself as a leader in secure digital transformation, balancing business growth, technological innovation, and data protection in an increasingly interconnected world.

The insights gained from this literature review provide the foundation for the next stage of this study. After identifying key gaps and challenges in GDPR compliance, data-privacy governance, and ERP implementation within the Indian context, the next chapter 3- Research Methodology describes how these issues are examined in practice. The next section also covers the research design, sampling process, and data-collection methods used to assess GDPR-readiness among Indian software implementation firms and to evaluate the proposed Privacy Assurance Framework.

CHAPTER III: RESEARCH METHODOLOGY

This chapter outlines the research methods adopted to investigate GDPR compliance challenges among Indian software package implementation companies. It begins with a description of the study problem, followed by the application of conceptual frameworks that guide the research. The chapter then details the mixed-methods research design, sample selection, and ethical considerations. It also explains the data collection tools and procedures, analysis strategies for both qualitative and quantitative data, and outlines the key limitations of the research design, including a comparative assessment of GDPR and India's DPDP Act to contextualize regulatory challenges.

3.1 Description of the Study Problem

The study examines the challenges faced by Indian software package implementation organizations in complying with GDPR, particularly when processing data for EU clients. Given GDPR's stringent data protection and privacy requirements, Indian companies must navigate complex regulatory landscapes to maintain both compliance and competitive advantage. The research aims to identify key hurdles, including gaps between local regulations and GDPR standards, and to propose strategies that enable these organizations to effectively manage cross-border data processing while aligning with both EU and Indian data protection frameworks.

3.2 Practical Application of Conceptual Frameworks

In this research, the theoretical constructs include GDPR compliance, DPIAs, and the economic implications of data privacy regulations. GDPR compliance is operationalized through the evaluation of organizational practices and policies against GDPR standards. DPIAs are assessed based on their implementation and effectiveness in identifying and mitigating privacy risks. The economic implications are measured by analyzing data on GDP growth in the Indian IT sector and correlating it with the presence or absence of robust data protection frameworks.

The independent variables in this study are EU-GDPR compliance and DPDP Act compliance, while the dependent variable is the level of data protection compliance achieved by Indian data processors. This operationalization will enable the study to systematically assess the alignment of data processing practices with GDPR.

The purpose of this research is to examine how Indian software package implementation companies can effectively align with GDPR requirements to support EU Clients. The research questions include:

3.3 Research Design

This research employs a mixed-methods approach, combining qualitative and quantitative techniques to provide a comprehensive analysis of GDPR compliance in Indian software companies. The qualitative aspect involves in-depth, semi structured interviews with data protecion officers, industry experts and company executives to gain insights into the practical challenges and strategies. As part of the quantitative component, many organisations will be surveyed using standardised questionnaires to collect the level of compliance and economic impact with the data. This technique analyses GDPR compliance-related subjective and objective data thoroughly.

3.4 Sample and Population

The participants for this research consists of software package implementation companies operating within India. This includes companies engaged in the development, customization, and deployment of software solutions for various business functions, including ERP systems, CRM systems, and other enterprise software solutions. The focus is on companies that have international operations or client bases, particularly those involved with European clients, due to the relevance of GDPR compliance.

The sample includes companies of varying sizes and sectors to confirm a complete considerate of the challenges and practices across different organizational contexts. A stratified random sampling technique is used to select participants, ensuring representation from small, medium, and large enterprises. The final sample comprises 50+ companies, selected based on their engagement with European clients and their relevance to GDPR compliance coverage.

3.4.1 Sampling design

The sampling design includes a comprehensive list of companies drawn from industry directories, professional associations, and business networks. This list is further refined to include only those companies actively involved in GDPR compliance or related regulatory activities. The sampling frame is created using data from sources such as the NASSCOM, the Indian CERT-IN and other industry-specific databases. The frame is frequently updated to reflect the most current and relevant companies engaged in GDPR compliance activities.

3.4.2 Sampling Method, Sample Size and Recruitment process

A stratified random sample ensures a representative sample across firm sizes and industries. This study splits the population into ERP packages (such Oracle, SAP, and MS Dynamics) and randomly selects samples from each, allowing for a more accurate representation and analysis of company category variances.

Statistical needs and practicality influence sample size. To balance statistical power and resource limits, the research samples 50+ organisations, 10+ from each Package implementation component. This guarantees dependable, manageable data collecting.

Emails to key contacts at chosen firms explaining the research aims and encouraging participation start the recruiting process (Dillman et al., 2014). Follow-up calls confirm interest and organise interviews or surveys. Call interviews may require participants to write out replies for record-keeping and validation. Sometimes surveys are done during the conversation in a call, depending on participant desire and availability. As an appreciation gesture, participants receive a summary of findings or industry publications with pertinent insights.

3.4.3 Ethical Considerations

The Consent form explains the research goal, data use, and participant rights (Belmont Report, 1979). Data is anonymised and kept securely to safeguard participant privacy. Personal identifiers that might directly attribute replies to people are not gathered, save for crucial professional identifiers pertinent to the study. The research follows ethical principles for confidentiality and integrity. Participation is voluntary, with the right to withdraw at any stage without consequences. Measures with restricted access to safeguard data ensure minimizing risks to participants. The study undergoes ethical review and approval to ensure compliance with established research standards.

3.4.4 Limitations of Sampling

Sampling has limits. If chosen firms do not participate, potential non-response bias may under-represent certain industry sectors or company sizes. Self-reported data also risks recollection bias and social desirability bias, where participants individuals may inadvertently misreport facts. In some cases, Participants may also be unwilling to reveal specific facts owing to confidentiality or regulatory concerns, which may compromise data accuracy. While Stratified random sample enhances representativeness, sampling frame limitations remain ,although industry directories and databases may not include all relevant organisations. Efforts such as follow-ups, secondary data validation, and ensuring diversity within the sample help mitigate these challenges, though some degree of bias may still be unavoidable.

3.5 Participant Selection

Participants are chosen for their GDPR compliance roles within their organisations. Inclusion criteria covers companies actively implementing software packages and serving European clientele are targeted. Exclusion criteria involve companies not operating within the specified sectors or those with insufficient scope on their GDPR practices. Selection is done through a combination of industry directories, recommendations from professional networks, and initial screenings to verify relevance and suitability.

Participants are typically senior managers, compliance officers, data protection officers (DPOs), leagal experts and IT professionals involved in GDPR implementation in various deparments within software prackage organisation, who process data relevan to scope of a natural person. This selection ensures that the data reflects the perspectives of individuals with relevant expertise and experience.

3.6 Data Collection Methods and Instrumentation

This study utilizes structured online surveys and semi-structured interviews as primary data collection instruments to assess GDPR compliance among Indian software package implementation companies. The structured online survey captures quantitative data on GDPR and DPDP compliance, privacy practices, awareness of data privacy risks and operational challenges faced by data processors in India.It consists of Likert-scale and multiple-choice questions, designed to measure regulatory awareness, implementation status, and compliance challenges. The survey instrument underwent a pilot testing with a small set of industry professionals to enhance validity ,while the interview guide consists of open-ended questions to explore compliance difficulties and industry best practices.

To complement the survey, semi-structured interviews provide qualitative insights into compliance challenges, industry best practices, GDPR implementation barriers and economic impacts. These interviews target Data Protection Officers (DPOs), compliance managers, and legal experts, using an open-ended interview guide to explore key compliance barriers and organizational strategies.

Data is collected via online surveys and call-based interviews, where participants may either complete survey responses post-interview for validation or fill out surveys during the call based on preference. Follow-ups are conducted to improve response rates. As a gesture of appreciation, participants receive a summary of research findings or industry insights relevant to their field.

3.7 Data Collection Procedures

Methodical data collection ensures validity and reliability. A stratified sample of software package installation professionals will get the structured survey online. This ensures a huge dataset on data processors' primary challenges, privacy practices, and GDPR compliance.

Semi-structured interviews with key stakeholders help understand GDPR implementation problems. The participants consent to our recording and transcription of interviews for study. Data collection includes participants verifying their replies following the interview.

To ensure data security and confidentiality, survey responses are anonymized, and all data is access restricted to authorized personnel. Ethical safeguard considerations include informed consent, GDPR-compliant privacy measures, and compliance with ethical research standards.

3.8 Data Analysis Strategies

This study uses quantitative and qualitative methodologies to examine GDPR and DPDP compliance in India's software package installation industry. This ensures economic impacts, industry issues, and compliance levels are recognised.

Quantitative analysis of structured online survey data will employ Minitab. We utilise descriptive statistics to summarise compliance levels and statistical hypothesis testing to find relationships between compliance processes and organisational variables. The key factors are determined using correlation and regression analysis. Economic statistics like its percentage of India's GDP will highlight the industry's importance and the necessity for stringent compliance.

In semi-structured interviews, DPOs, compliance managers, and legal experts will be interviewed. The data will be thematically coded to find patterns and insights. This will help investigate GDPR implementation challenges, industry readiness, and privacy assurance strategies. This study will use quantitative and qualitative data to illuminate GDPR compliance trends, operational challenges, and economic issues. With insights, an Indian software industry-specific Privacy Assurance Framework based on the EU General Data Protection Regulation will be created.

Before performing statistical analysis, the collected dataset underwent a thorough cleaning and validation process. Incomplete or duplicate responses were excluded, and only 158 verified entries were retained for analysis. The cleaning step ensured consistency across demographic variables and response categories, reducing bias and enhancing the accuracy of descriptive and regression analyses presented in next chapter. These procedures contributed to the overall reliability and validity of the study’s empirical findings.

3.9 Limitations of Research Design

A fair evaluation of a research work requires acknowledging its limitations. These minor limits must be addressed to understand the study and its outcomes. These constraints may limit the study's

scope, applicability, and impact, especially given India's software package installation business's GDPR compliance. These limitations must be acknowledged to better future research and coordinate legislative actions.

3.9.1 Key Limitations

- **Reliance on Self-Reported Data**

Sector stakeholders self-report data, which potentially bias this study. Instead of being honest about GDPR compliance, responders might provide socially acceptable answers. Business spokespeople may minimise or exaggerate GDPR compliance due to image concerns.While efforts have been made to cross-validate responses with secondary data sources, independent reports, and regulatory findings, complete mitigation of self-reporting bias remains a challenge for consideration.

- **Sample Size and Representation**

Although the study aims to capture a diverse representation of software companies implementing GDPR frameworks in India, the sample size may not fully reflect the industry's entire compliance landscape. Small and medium-sized enterprises (SMEs) may have different constraints compared to multinational corporations, and variations across industry sub-sectors may not be fully accounted for. A larger and more diversified sample in future studies could help enhance generalizability and provide a more holistic picture.

- **Legislative Specificities and Applicability to Other Regions**

This research focuses primarily on EU GDPR and its comparison with India’s legislative landscape, considering India’s Digital Personal Data Protection (DPDP) Act. Given the jurisdictional focus, findings may not be fully applicable to other regulatory environments such as the United States (CCPA), China’s PIPL, Singapore’s PDPA or Brazil’s LGPD. Each country has distinct legal frameworks and compliance requirements, making it necessary to contextualize findings when applying them outside of India.

- **Company-Specific Variations in GDPR Compliance**

The software package implementation industry is highly diverse, with companies adopting GDPR compliance at different levels based on business models, client expectations, and risk tolerance. While large organizations may have dedicated data protection teams, smaller firms may struggle with implementation due to budgetary and workforce constraints. The study’s recommendations may not be universally applicable, as operational, technical, and financial realities vary significantly among firms.

- **Effectiveness of Compliance Mechanisms**

This study assumes that GDPR adoption improves data protection standards in India, However, real-world implementation may be influenced by several factors:

- Regulatory gaps that enable firms to demonstrate compliance on paper without robust enforcement mechanisms.
- Inconsistent enforcement by Indian regulatory bodies compared to the stricter oversight of EU institutions.
- Challenges in adapting GDPR requirements to existing workflows, leading to integration difficulties for firms.

Future studies could examine post-implementation compliance audits to assess how effectively companies implement GDPR principles beyond initial adoption.

- **Skill Gaps in Data Protection Roles**

The effectiveness of GDPR compliance depends on the competency of data protection officers (DPOs) and Privacy Practitioners. However, India faces skill shortages in cybersecurity, legal compliance, and privacy governance. Many organizations may lack trained personnel, leading to improper implementation or partial compliance. Establishing certification programs, standardized GDPR training, and capacity-building initiatives could address this issue.

- **Dynamic Nature of Data Protection Regulations**

Both GDPR and India's DPDP Act are evolving legal frameworks. Amendments, judicial interpretations, or new data-sharing policies could impact the study's findings. For example, the EU has introduced the AI Act and Data Governance Act, which may introduce further compliance complexities. The regulatory landscape's constant evolution necessitates periodic reviews of compliance frameworks to ensure relevance.

- **Access to Confidential Information**

Data privacy is a sensitive domain, and organizations may withhold detailed compliance reports, internal audits, or data breach incidents due to confidentiality concerns. This limitation affects the depth of analysis regarding real-world GDPR violations, enforcement actions, and compliance gaps. Future research could benefit from government-released compliance audits or whistleblower reports to gain deeper insights.

- **Industry-Specific Challenges**

The proposed Privacy Assurance Framework tailored to the Indian software package implementation industry may not fully address unique industry challenges, such as:

- Challenges in vendor compliance, as third-party software providers may not fully adhere to GDPR requirements.
- Complex contractual obligations, particularly in offshore development models that involve cross-border data processing.
- Sector-specific variations in data handling, as compliance requirements differ across industries such as fintech, healthcare, and e-commerce.

A sector-specific analysis could offer more targeted recommendations, ensuring that GDPR and DPDP Act compliance strategies are tailored to the unique regulatory and operational needs of different software organizations.

- **Resource Constraints for SMEs**

Small and mid-sized enterprises (SMEs) of Indian ERP implementation organizations may lack the financial and human resources required to implement GDPR fully. Compliance involves:

- Hiring DPOs, Privacy Practitioners and legal experts.
- Updating IT infrastructure to support GDPR mandates.
- Conducting regular compliance audits.

These requirements can be cost-prohibitive, making it necessary for policymakers to consider financial incentives, subsidies, or phased compliance models for SMEs.

- **Awareness and Training Gaps**

GDPR compliance is not just a legal framework but also an organizational culture transformation challenge. Many firms struggle with employee awareness, training, and operational compliance. However, Establishing standardized GDPR training programs, government-backed awareness initiatives, and sector-specific guidelines could bridge this gap.

- **Interoperability with Existing Systems**

Many organizations rely on legacy IT systems that were not originally designed to meet GDPR requirements. Integrating compliance mechanisms into these systems presents several challenges, including:

  - Significant investment in modern data management software to ensure Privacy and regulatory compliance.

- Re-engineering existing workflows to align with GDPR principles, potentially disrupting established processes.
- Comprehensive employee training on new compliance procedures to mitigate risks of non-compliance and breaches.

These operational shifts can lead to disruptions, implementation delays, and cost overruns, making GDPR adaptation a complex and resource-intensive process for organizations.

- **Vendor and Client Alignment Challenges**

Ensuring that software vendors, clients, and third-party service providers align with GDPR requirements presents significant challenges. Variations in contractual obligations, regional compliance standards, and enforcement mechanisms can create compliance gaps and legal ambiguities. To mitigate these risks, companies must:

- Establish comprehensive data protection agreements with all stakeholders to ensure accountability.
- Standardize compliance frameworks to bridge regulatory differences across jurisdictions.
- Implement robust compliance monitoring, privacy assessment and auditing mechanisms to track vendor and partner adherence to GDPR.

Without well-defined contractual safeguards and enforcement strategies, organizations may face gaps in compliance, increasing the risk of regulatory violations, legal disputes, privacy breaches and financial penalties. Establishing clear accountability measures and ensuring consistent enforcement across all stakeholders is essential for maintaining GDPR compliance.

- **International Collaboration Constraints**

Given that many Indian firms serve EU-based clients, GDPR compliance is crucial for sustaining business relationships and market credibility. However, several factors can hinder full-scale GDPR adoption, including:

- Legal and diplomatic negotiations over data transfer frameworks and compliance certifications.
- Uncertainties in enforcement reciprocity, as differences in regulatory frameworks between India and the EU create challenges in ensuring consistent compliance monitoring, penalty enforcement, and legal accountability across jurisdictions.
- Delays in implementing standardized compliance mechanisms due to differing national regulations.

Proactive regulatory harmonisation, cross-border coordination, and intentional policy interventions are needed to help Indian package firms serving EU clients shift smoothly.

3.9.2 Comparative Limitations: DPDP Act vs. GDPR

While GDPR is designed to provide a high level of data protection and privacy, the DPDP Act, which represents a forward step for India in data privacy standards, may have differences and potentially weaker aspects compared to GDPR. Although The DPDP Act is focused to improve India's data protection and privacy, the Act is Indian-specific and may need to evolve to meet international standards. The DPDP Act and GDPR both aim to safeguard privacy and data, although they may differ and be weaker. The DPDP Act advances Indian data protection and privacy laws(DR. Reeta, 2023). However, the DPDP Act is Indian-specific and may evolve to meet international standards. As shown in Table 8 below, the DPDP Act's weaknesses compared to the EU General Data Protection are:

Table 8: Comparison of GDPR vs. DPDP

Aspect	GDPR	DPDP Act 2023
Legal Basis	EU Regulation	Indian Legislation
Applicability	European Union Member States	India
Extraterritorial Application	Yes, applies globally if processing EU residents' data	It is applicable worldwide if they are selling products or services to people in India.
Data Subject Rights	Robust data subject rights	Rights of access, correction, and deletion for individuals
Data Protection Officer Requirement	Mandatory for certain organizations	Required for data fiduciaries
Data Transfer Restrictions	Stringent transfer restrictions	Restrictions on data transfer to certain countries
Consent Requirements	Specific, informed, and unambiguous consent	Free, unambiguous, clear affirmative action consent
Fines for Non-Compliance	Twenty million euros, or four percent of yearly global sales	Up to 250 crores INR or 4% of global turnover, either is higher
Enforcement Authority	Various supervisory authorities for regions	Data Protection Board of India
Data Localization Requirements (within country)	No – Covered in overall framework	Absolutely, we will only store sensitive personal data in India.

Source: (Chaturvedi and Sinha, 2017)

- **Fines and Penalties**

GDPR fines are harsher than DPDP Act fines. Fines under the DPDP Act cannot exceed INR 15 Crore (€1.75 million Max), but GDPR fines can reach 4% of worldwide sales or €20 million Max. Please refer to Table 9 below for a detailed comparison of DPDP Act vs GDPR Fines.

Table 9:GDPR vs. DPDP Fines (with Currency equivalents for comparison)

Violation Description	GDPR Fine (EUR)	DPDP Fine (INR)	Approx. in EUR / USD
Data breach with delayed notification	€20 million or 4% of global annual turnover (whichever is higher)	Up to ₹250 crores	~€27.8 million / ~$30 million
Violation of data subject rights	€20 million or 4% of global annual turnover (whichever is higher)	Up to ₹200 crores	~€22.2 million / ~$24 million
Non-compliance with principles/obligations	€10 million or 2% of global annual turnover (whichever is higher)	Up to ₹100 crores	~€11.1 million / ~$12 million
Violation of consent and processing conditions	€20 million or 4% of global annual turnover (whichever is higher)	Up to ₹250 crores	~€27.8 million / ~$30 million
Failure to cooperate with authorities	€10 million or 2% of global annual turnover (whichever is higher)	Up to ₹100 crores	~€11.1 million / ~$12 million
Unauthorized international data transfers	€20 million or 4% of global annual turnover (whichever is higher)	Up to ₹250 crores	~€27.8 million / ~$30 million
Lack of Data Protection Impact Assessment (DPIA)	€10 million or 2% of global annual turnover (whichever is higher)	Up to ₹100 crores	~€11.1 million / ~$12 million
Default/design flaws in data protection	€10 million or 2% of global annual turnover (whichever is higher)	Up to ₹100 crores	~€11.1 million / ~$12 million

Source: (Kuner, 2020)

Note: Currency conversions are approximate and based on average exchange rates as of September 2025 — €1 = ₹90 and US $1 = ₹83. Values are rounded to the nearest €0.1 million / US $0.1 million for ease of comparison. Actual penalty impacts may vary with exchange-rate fluctuations and applicable turnover calculations under respective regulations.

- **Data Subject Rights**

While the DPDP Act grants data subject rights, including the right to access and correction, GDPR provides a more comprehensive set of rights, including data portability, the right to be forgotten, and more.

- **Cross-Border Data Transfer**

GDPR has strict rules for international data transfers, including the use of SCCs and binding corporate rules. DPDP Act allows data transfer to any country unless restricted by the Central Government, potentially leading to varying standards of protection.

- **Data Breach Notifications**

GDPR mandates data break notifications within 72 hours of flattering alert of a breach. DPDP Act does not specify a specific timeframe, potentially allowing for delays in reporting.

- **Data Protection Officers (DPOs)**

GDPR commands the appointment of DPOs in particular cases, ensuring expertise in data protection. DPDP Act has similar provisions but may not have stringent requirements for DPOs.

- **Independent Supervisory Authority**

While GDPR creates independent guiding authorities in each EU associate state to enforce data protection laws, the DPDP Act envisions an independent Data Protection Board but also grants significant power to the Central Government, potentially affecting its independence.

- **Consent Requirements**

GDPR sets high standards for obtaining consent, including clear and unambiguous consent. DPDP Act may have different consent requirements.

- **Territorial Scope**

The GDPR establishes defined roles for independent supervisory bodies, while the DPDP Act provides the federal government broad jurisdiction, which might impair enforcement and monitoring.

- **Data Transfer Mechanisms**

GDPR provides specific mechanisms for data transfers, such as SCCs and binding corporate rules. DPDP Act lacks detailed provisions on these mechanisms.

- **Enforcement and Oversight**

The GDPR establishes defined roles for independent supervisory bodies, while the DPDP Act provides the federal government broad jurisdiction, which might impair enforcement and monitoring.

- **Over-Broad Surveillance**

Critics argue that the DPDP Act does not contain meaningful safeguards against over broad surveillance, potentially compromising individuals' privacy and civil liberties.

- **Concerns about Data Processing Over Privacy**

The DPDP Act has been criticized for prioritizing data processing over privacy, violating its declared objective of preserving individual's rights and personal data.

India's data privacy policy framework needs urgent improvements. This framework should take into account the software package implementation industry's particular peculiarities and conform with globally recognized standards like the EU-GDPR. Each constraint in this chapter emphasizes the need for long-term data protection and the need to treat unique issues thoughtfully, emphasizing the importance of implementing sustainable data protection measures. This recognition should encourage Indian regulatory authorities, industry stakeholders, policy makers and legislators to collaborate on a contemporary data protection framework that meets the country's needs. Failure to enhance GDPR compliance within Indian software package implementation companies not only risks losing trust with global clients and compromising privacy but also threatens the sector's economic significance, necessitating urgent action to address the identified limitations and foster a deeper understanding of GDPR compliance in the industry.

3.10 Conclusion

This methodology section uses a strong mixed-methods approach to examine comprehensive analysis of GDPR compliance in Indian software package implementations companies. The research will use quantitative surveys and qualitative interviews to address the issues and provide practical insights. The selected methods analyse how companies in India's software package implementation business manage expanding data protection laws, assessing both the practical and economic aspects of GDPR compliance. The key outcome of this study is the development of a GDPR-based Privacy

Assurance Framework formulated for Indian data processors. As outlined in Section 1.5, this framework is not a proposal for new or unified legislation but an operational model designed to enhance alignment between the EU GDPR and India’s DPDP Act. Strengthening this alignment India's data governance, regulatory compliance, and worldwide reputation in global markets. The industry's importance in India's digital economy requires strong data protection for economic growth and international links. However, Operational, legal, regulatory and industry specific issues hinder a smooth implementation.

The DPDP Act and GDPR differ significantly in regulation and execution gaps. DPDP Act enforcement is laxer, sanctions are lower, and Indian data subjects have less rights than GDPR. GDPR has stronger fines, greater data subject rights, and impartial assessment, but the DPDP Act's government-centric regulatory framework may affect data privacy with weaker enforcement, lower fines and limited data subject rights. Furthermore, Infrastructural constraints, uninteroperable systems, a shortage of experienced staff, and financial responsibilities on SMEs hinder full compliance.

Despite these challenges, This study shares useful insights by examining compliance readiness, industry restrictions, and strategic recommendations to align India's data protection system with global standards. This study has some limitations. This includes self-reported data bias, a limited sample size, and lack of access to sensitive company data. When evaluating the data, these factors may impact how they are applied to a broader context.

In the next chapter, We move forward to data analysis, where we closely examine India's software package installation market and how companies comply with GDPR and DPDP Act. This study will analyse compliance trends, legislative impediments, and industry readiness, this analysis will identify critical vulnerabilitues and propose actionable strategies to help India develop a globally competitive, GDPR-aligned data protection framework. The study aims to assist firms develop a GDPR-compliant, globally competitive, and adaptable data governance system.

CHAPTER IV: DATA ANALYSIS

This chapter presents the analysis of quantitative and qualitative data collected through surveys and interviews on ERP usage, regulatory compliance, and data privacy practices among Indian offshore software providers. It identifies key trends, relationships, and compliance challenges with respect to GDPR and the DPDP Act. The findings provide the empirical foundation for developing the Privacy Assurance Framework proposed in the next chapter.

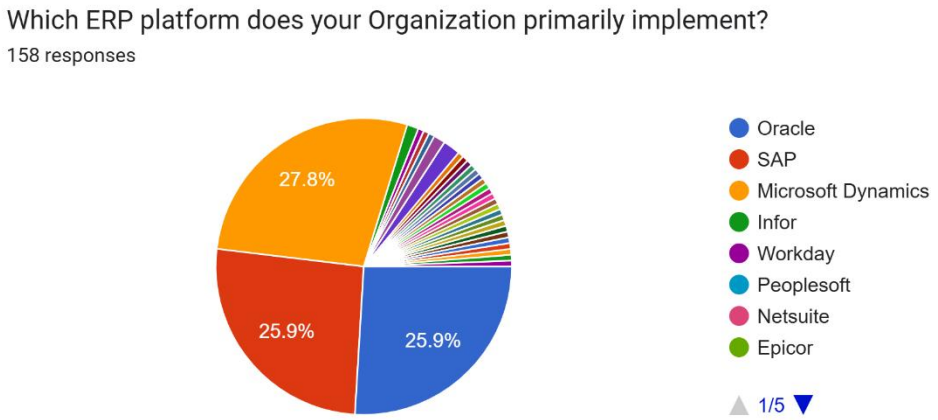
4.1 Introduction

This chapter analyses 158+ survey responses on ERP platform utilisation, geographical market distribution, module uptake, compliance awareness, team sizes, and organisational difficulties. The findings underscore India's status as a prominent offshore service provider by focussing on Indian enterprises that deploy software package solutions for European and North American clients. Microsoft Dynamics, SAP, and Oracle dominate ERP implementations, while smaller solutions serve specific industries. Oracle excels in finance, SAP in HRM, and Microsoft Dynamics in CRM. Due to awareness, resource limits, and legal complexity, many organisations are not complying with GDPR and DPDP Act. Team sizes, DPO presence, and privacy framework implementation are also shown. These findings help uncover industry-wide compliance issues and data governance opportunities in India's software package implementation business.

4.2 Analysis Summary and interpretation

This section examines survey responses, focusing on ERP adoption, regional market distribution, GDPR and DPDP Act compliance, and key organizational challenges. The findings provide insights into industry preparedness and data protection practices.

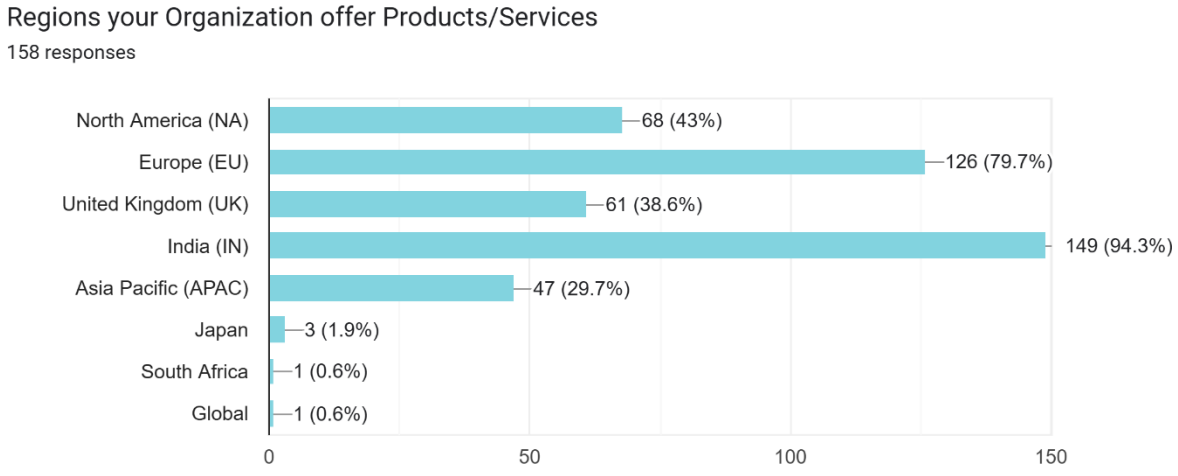
Figure 7: Platform Adoption Distribution Across Organizations



Source: Author's own analysis

A distribution chart for ERP platforms used by various businesses was created from 158+ replies. Most implementations (27.8%) are Microsoft Dynamics. SAP and Oracle trail with 25.9% each, demonstrating their ERP industry dominance. Few respondents (20.4%) utilized Infor, Workday, Peoplesoft, NetSuite, or Epicor. Infor and Workday stand out with 6.3% and 4.4%. Epicor is 1.3%, Peoplesoft 2.5%, and NetSuite 2.5%. ERP solutions are used on a wide range of smaller platforms (3.4%). Even though the three main platforms dominate the market, smaller ERP systems are employed to meet unique organizational or sector needs, according to the statistics.

Figure 8: Geographic Coverage of Products and Service Offerings

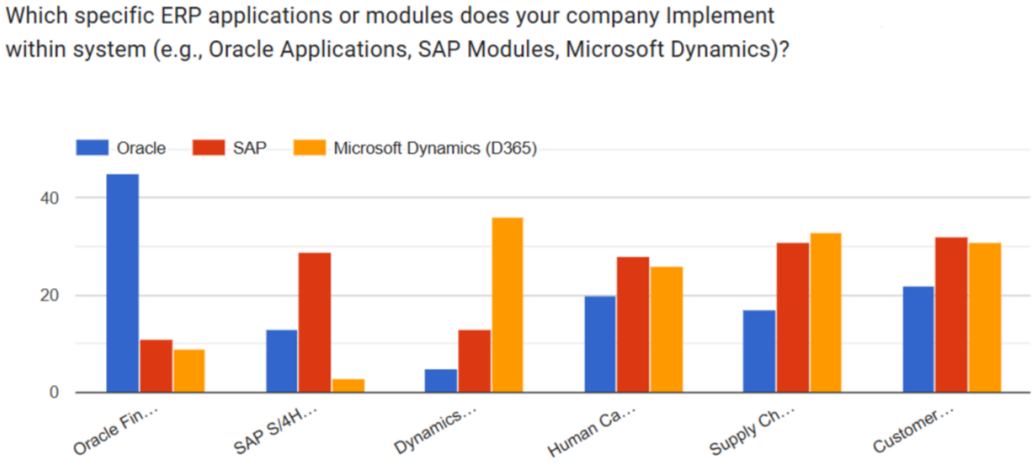


Source: Author's own analysis

Note: *As respondents could select multiple regions, the cumulative percentage exceeds 100%. Figures represent the proportion of respondents selecting each region.*

The chart shows the regional distribution of products/services offered by organizations, based on 158+ responses. It is important to note that respondents could select multiple regions, which is why the cumulative percentage exceeds 100%. India leads significantly with **149 responses (94.3%),** followed by Europe at **126 responses (79.7%).** North America and the United Kingdom are also key markets, with **68 responses (43%)** and **61 responses (38.6%),** respectively. The Asia Pacific region accounts for **47 responses (29.7%),** while Japan has a modest presence at **3 responses (1.9%)**. South Africa and global markets each received **1 response (0.6%),** indicating minimal presence. These ratios highlight India's dominant role as a global service provider while showcasing overlapping international footprints.

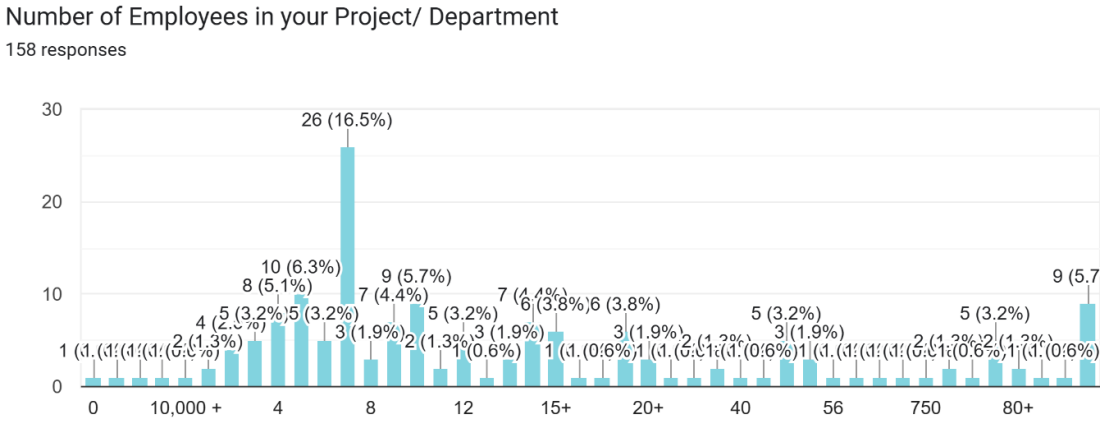
Figure 9:Cross-Platform Adoption Trends of ERP Functional Modules



Source: Author's own analysis

From 158+ responses, this figure shows Oracle, SAP, and Microsoft Dynamics (D365) ERP application or module usage percentages. Oracle Financials was the most widely implemented module with 25.3% of replies. The next most popular ERP system is SAP S/4HANA (19%). The most popular CRM software is Microsoft Dynamics CRM with 25.3% market share. SAP dominates human capital management with 22.2%. MS Dynamics is second with 19%, followed by Oracle with 15.8%. While Oracle is third with 15.8% in Supply Chain Management, SAP and Dynamics tie for first with 19%. CRM use is evenly distributed across platforms, with 19% of deployments on each. This distribution illustrates that module choices vary: Oracle rules finance, SAP rules human capital management, and Dynamics rules customer relationship management.

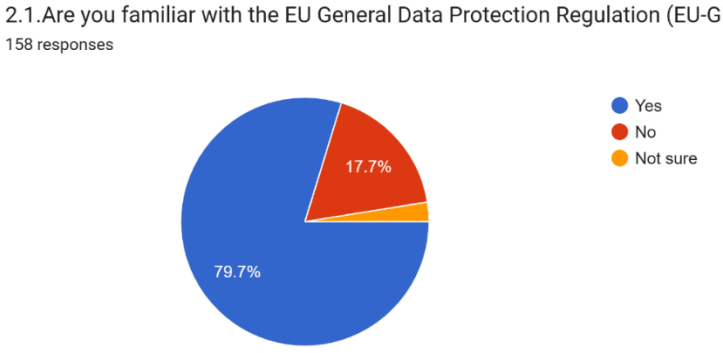
Figure 10: Distribution of Workforce Size Across Surveyed Projects and Departments



Source: Author's own analysis

This bar graph shows the distribution of employees across numerous project or department sizes, based on 158+ responses. The most common department size is 4 employees, representing 16.5% (26 responses). The next most common sizes are 8 employees and 80+ employees, both at 5.7% (9 responses each). Departments with 10 employees account for 6.3% (10 responses). Smaller teams, such as those with 2 or 5 employees, each represent 3.2% of the total (5 responses each). The least frequent team sizes are 1 employee, occurring only 1 time or 0.6%. Large teams, like those with 750 or 10,000+ employees, also account for 0.6% (1 response). These results indicate a significant skew towards smaller team sizes, with a sharp peak at 4 employees and smaller peaks at larger sizes, showing diverse team distributions across projects and departments.

Figure 11: Awareness levels of the EU General Data Protection Regulation among respondents

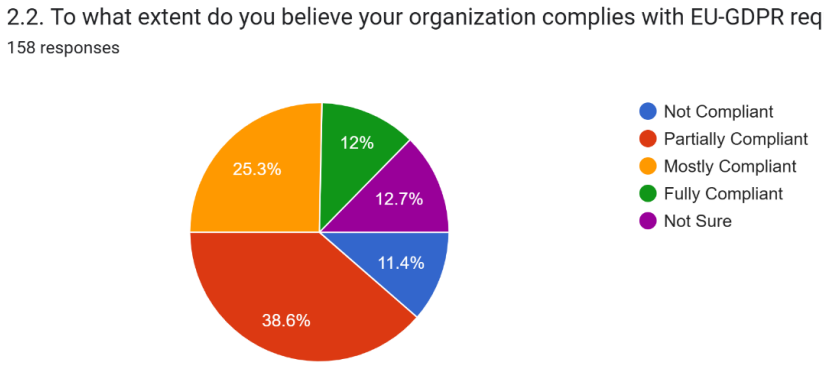


Source: Author's own analysis

In this survey 79.7% of the participants are familiar with EU-GDPR, 17.7% of the participants are not familiar with EU-GDPR and 2.6% of the participants are not sure about EU-GDPR. This high

level of unfamiliarity and uncertainty (over 20% combined) is notable, especially given the regulation's global relevance. This gap may stem from limited awareness campaigns, lack of formal training, or insufficient exposure to international regulatory standards among smaller or domestically focused firms. Educational background, organizational role, and lack of data governance responsibilities may also contribute to this discrepancy in familiarity.

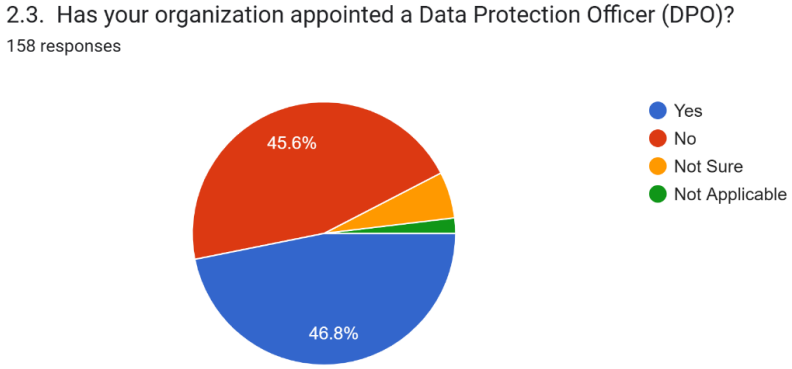
Figure 12: Survey Insights on Organizational Readiness for GDPR Compliance



Source: Author's own analysis

In this survey, the largest portion, 38.6%, believe their organization is partially compliant, while 25.3% view it as mostly compliant. 12.7% are unsure about the compliance status, and 11.4% consider their organization not compliant. Only 12% believe their organization is fully compliant. These results highlight a significant gap in full GDPR compliance awareness, with the majority either uncertain or identifying partial compliance, indicating room for improvement in organizational data protection measures as an Indian service provider.

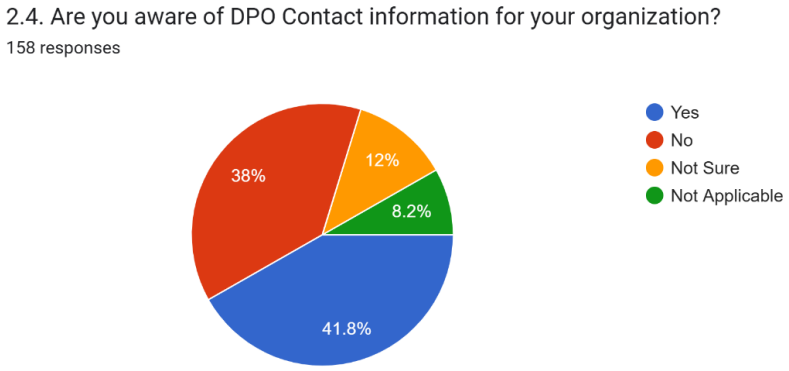
Figure 13: Organizational Adoption of Data Protection Officer (DPO) Roles



Source: Author's own analysis

According to this survey, 46.8% of the participants organization appointed Data Protection Officer (DPO), 45.6% of the participants organization didn't appoint a DPO, 2.8% of the participants not sure about organization appointed DPO and 1% of the participants said that DPO is not applicable in their organization.

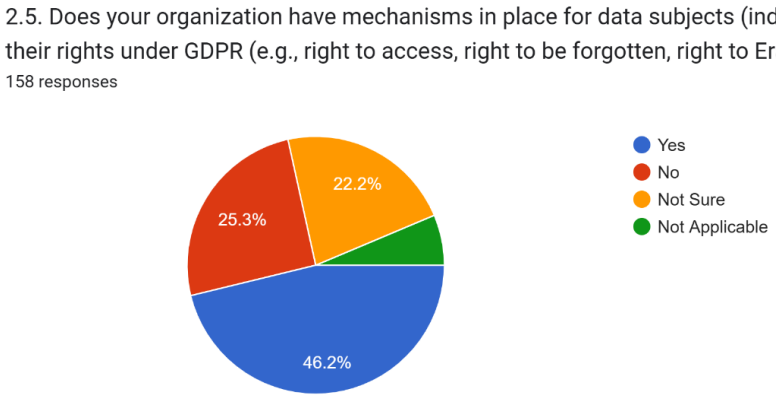
Figure 14: Awareness Levels of DPO Communication Channels Among respondents



Source: Author's own analysis

In this survey, 41.8% of the participants are aware of DPO Contact information for their organization, 38% of the participants are not aware of DPO Contact information for their organization, 12% of the participants are not sure about the awareness towards DPO Contact information for their organization and 8.2% of the participants shared not applicable for DPO Contact information for their organization.

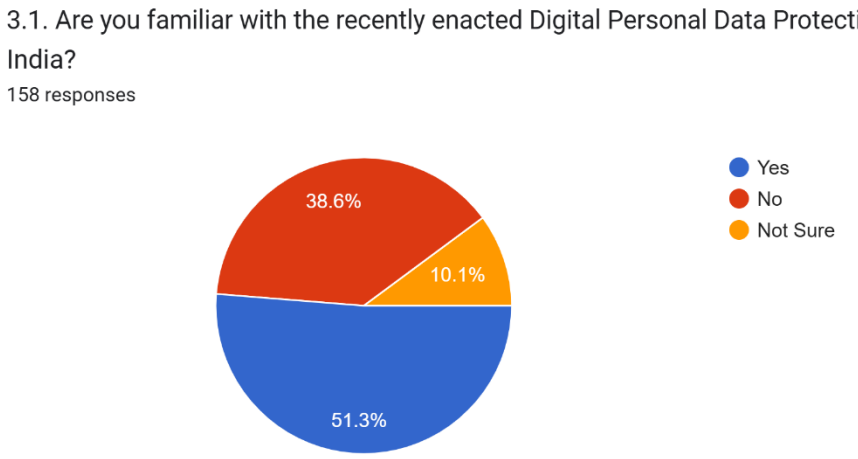
Figure 15: Organizational Readiness in Facilitating Data Subject Rights Under GDPR



Source: Author's own analysis

The pie chart illustrates the status of GDPR mechanisms in organizations based on 158+ responses. A significant **46.2%** confirm that their organizations have mechanisms in place to allow individuals to exercise their GDPR rights. However**, 25.3%** state their organizations do **not** have such mechanisms, while **22.2%** are **not sure.** A smaller portion, **6.3%,** find these mechanisms **not applicable**. This indicates that while nearly half of the organizations are compliant in this aspect, a notable proportion either lacks these mechanisms or has unclear awareness about their privacy controls implementation.

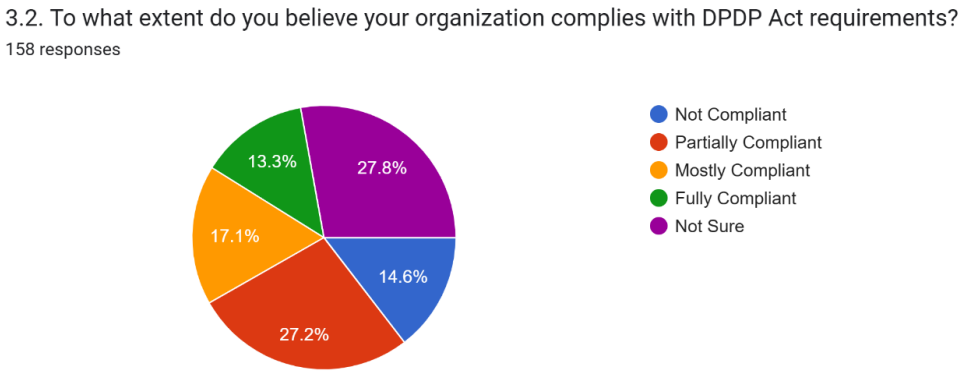
Figure 16: Respondent Familiarity with India's Digital Personal Data Protection Act



Source: Author's own analysis

In this survey, 51.3% of the people says yes that they are familiar with the recently enacted India's DPDP Act (2023).38.6% of the people says no, that they are not familiar with the recently enacted DPDP Act (2023) in India.10.1% of the people says that they are not sure with the recently enacted DPDP Act (2023) in India.

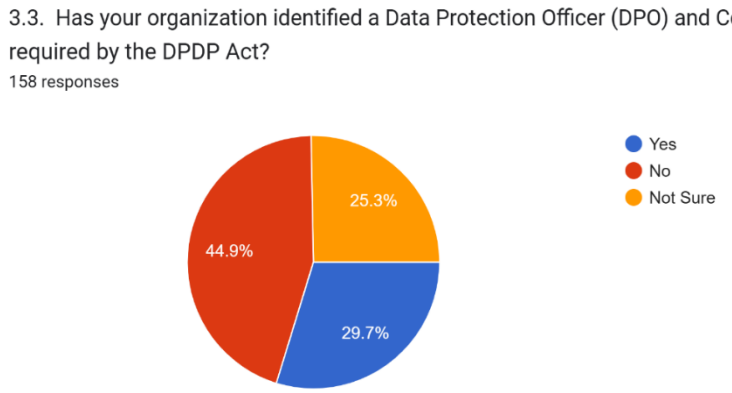
Figure 17: Distribution of Organizational Compliance Maturity Under the DPDP Act



Source: Author's own analysis

In this survey, 27.8% of the people say that they are not sure if their organization complies with DPDP Act requirement.27.2% of the people say that their organization is partially compliant with DPDP Act requirement.17.1% of the people say that their organization is mostly compliant with DPDP Act requirement.14.6% of the people say that their organization is not compliant with DPDP Act requirement.13.3% of the people say that they are fully compliant towards organization's compliance with DPDP Act requirement.

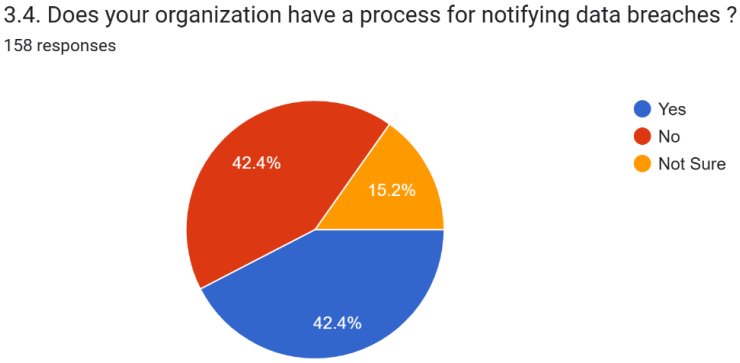
Figure 18: Adoption of DPO and Consent Management Roles Across Organizations



Source: Author's own analysis

In this survey, 29.7% of the people says "yes" that the organization has identified a data protection officer (DPO) and consent manager roles as required by the DPDP Act.44.9% of the people says no that the organization has not identified a data protection officer (DPO) and consent manager roles as required by the DPDP Act. 25.3% of the people are not sure if the organization has identified a data protection officer (DPO) and consent manager roles as required by the DPDP Act.

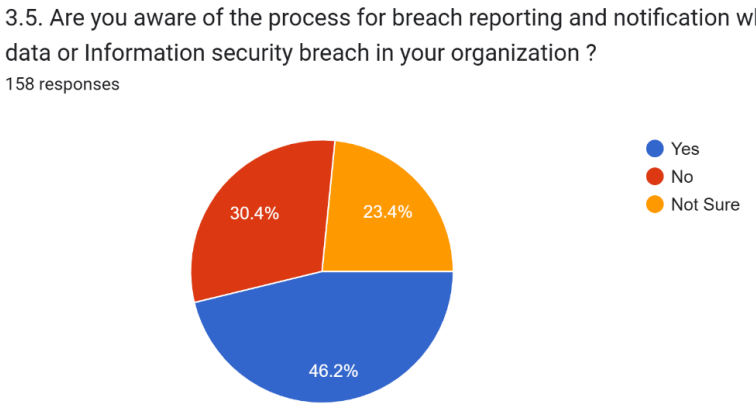
Figure 19: Organizational Readiness in Implementing Data Breach Notification Protocols



Source: Author's own analysis

In this survey 42.4% of the people says 'yes' that their organization has a process for notifying data breaches. 42.4% of the people say no that their organization does not have a process for notifying data breaches. 15.2% of the people say they are not sure about their organization towards having a process for notifying data breaches.

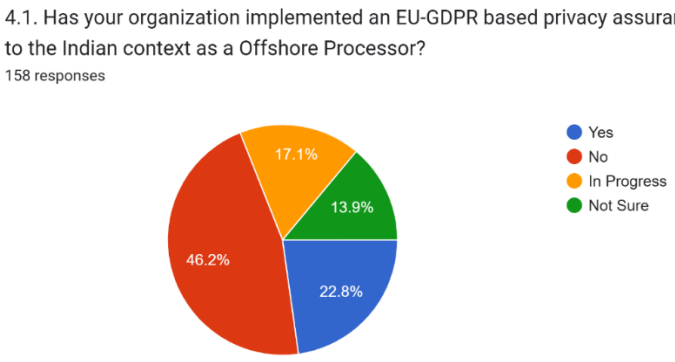
Figure 20: Awareness of Breach Reporting and Notification Processes Among respondents



Source: Author's own analysis

In this survey, 46.2% of the people says 'yes' that they are aware of the process of breach reporting and notification when they come across a data or information security breach in their organization. 30.4% of the people say no that they are not aware of the process of breach reporting and notification when they come across a data or information security breach in their organization. 23.4% of the people say they are not sure about aware of the process for breach reporting and notification when they come across a data or information security breach in their organization.

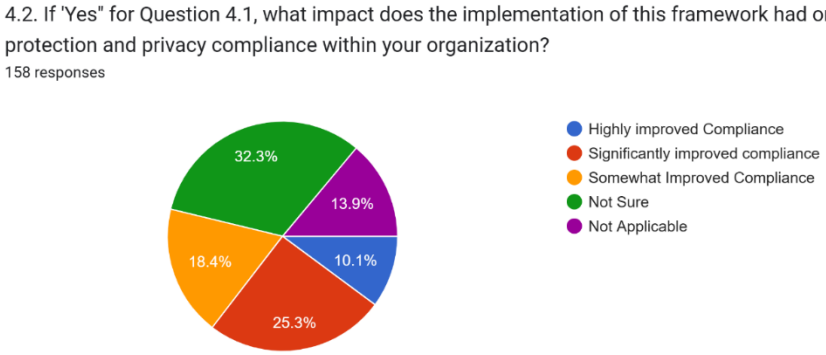
Figure 21: Survey Insights on GDPR Privacy Framework Among Indian Offshore Processors



Source: Author's own analysis

In this survey, 22.8% the people says ‘yes’ that their organization implemented an GDPR based privacy assurance framework tailored to the Indian context as an offshore processor. 46.2% the people says no that their organization have not implemented an GDPR based privacy assurance framework tailored to the Indian context as an offshore processor. 17.1% the people says that their organization is in progress for implementing an GDPR based privacy assurance framework tailored to the Indian context as an offshore processor. 13.9% the people says they are not sure/ not aware that their organization have implemented an GDPR based privacy assurance framework tailored to the Indian context as an offshore processor.

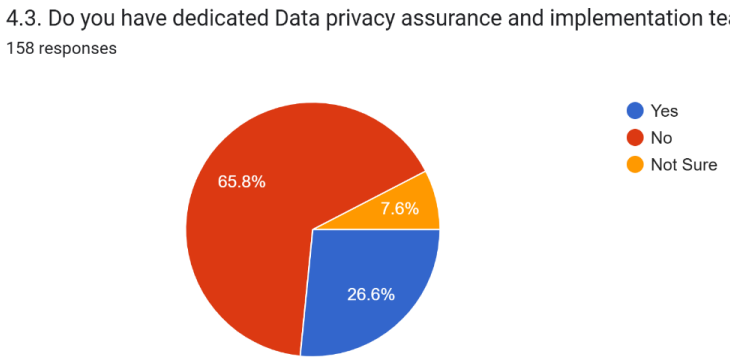
Figure 22: Perceived Improvements in Data Protection and Privacy Compliance implementation



Source: Author’s own analysis

In this survey, 10.1% of people say that implementation of GDPR based framework have highly improved compliance as an impact of the implementation towards data protection and privacy compliance within their organization. 13.9% of the people say it is not applicable towards implementation of GDPR based framework on data protection and privacy compliance within their organization. 18.4% of the people say that the framework implementation has somewhat improved compliance towards data protection and privacy compliance within their organization. 25.3% of the people says that the framework has significantly improved compliance towards data protection and privacy compliance within their organization. 32.3% of the people say they are not sure or not aware of the implementation of this framework towards data protection and privacy compliance within their organization.

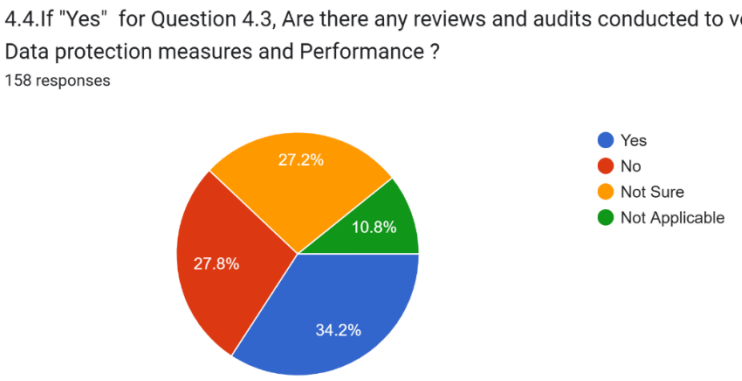
Figure 23: Availability of Dedicated Teams for Data Privacy Assurance and Implementation



Source: Author's own analysis

In this survey, 26.6% of the people say 'yes' that they have dedicated data privacy assurance and implementation team in their organization. 65.8% of the people says no that they do not have a dedicated data privacy assurance and implementation team within their organization. 7.6% of the people says not sure/not clear about having dedicated data privacy assurance and implementation team within their organization.

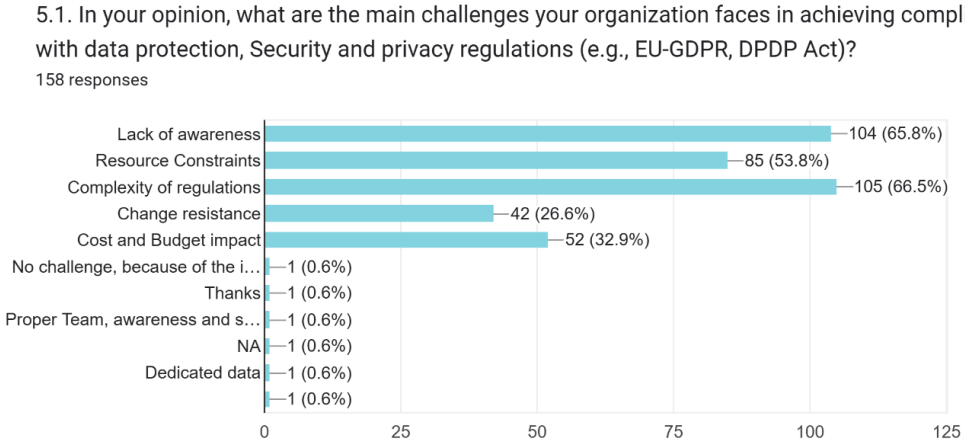
Figure 24: Survey Insights on Audit Processes for Evaluating Data Protection performance



Source: Author's own analysis

In this survey, 34.2% of the people say yes to the review and audits conducted to verify compliance for data protection measures and performance. 27.8% of the people says no to the review and audits conducted to verify compliance for data protection measures and performance. 27.2% of the people says not sure about the review and audits conducted to verify compliance for data protection measures and performance, 10.8% of the people says not applicable to the review and audits conducted to verify compliance towards data protection measures and performance.

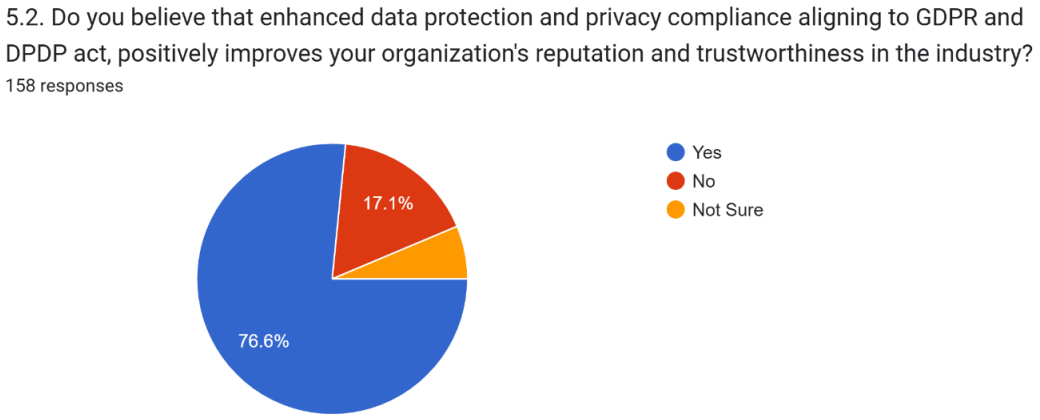
Figure 25: Survey Insights on Challenges Impacting Organizational Compliance with Privacy Frameworks



Source: Author's own analysis

In this survey considering the top 5, 65.8% of the people says that the main challenge for their organization in achieving acquiescence with data safety, security and privacy regulations is lack of awareness, 53.8% of the people says that the main challenge for their organization in achieving compliance with data protection, security and privacy regulation is resource constraints, 66.5% of the people says that the main challenge for their organization in achieving compliance with data protection, security and privacy regulation is complexity regulation. 26.6% of the people says that the main challenges for their organization in achieving acquiescence with data safety, security and privacy regulation is change resistance, 32.9% of the people says that the main challenge for their organization in achieving compliance with data protection, security and privacy regulation is cost and budget impact and the remaining least participants highlight that the main challenges for their organization in achieving compliance with data protection, security and privacy regulation is proper team awareness and dedicated data.

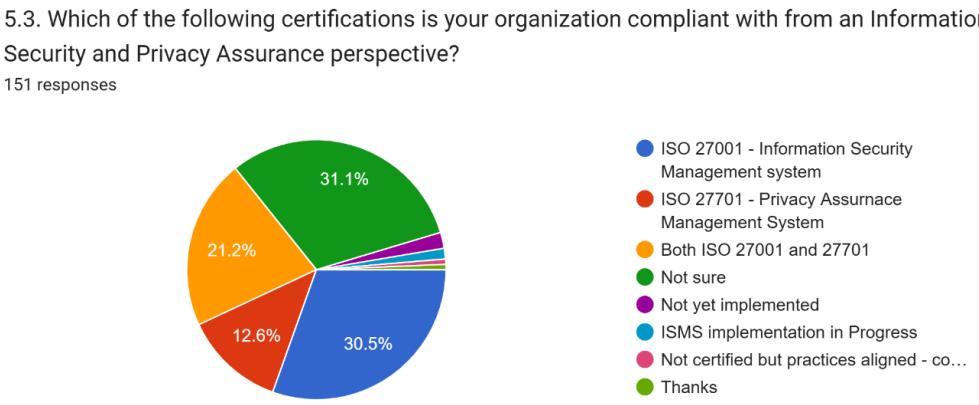
Figure 26: Influence of Enhanced Data Protection Compliance on Organizational Trustworthiness



Source: Author's own analysis

In this survey, 76.6% of the people say 'yes' that they believe that enhanced data protection and privacy compliance aligning to GDPR and DPDP act positively improve their organization reputation and trustworthiness in the industry. 17.1% of the people say 'no' that they believe that enhanced data protection and privacy compliance aligning to GDPR and DPDP act does not positively improve their organization reputation and trustworthiness in the industry. The remaining population of the people say that they are not sure or not aware if enhanced data protection and privacy compliance aligning to GDPR and DPDP act positively improve their organization reputation and trustworthiness in the industry.

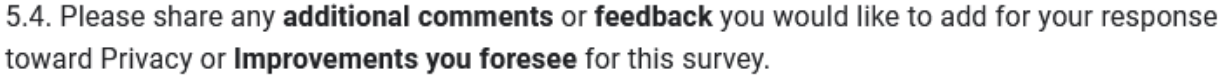
Figure 27: Survey Insights on Certification Alignment for Information Security and Privacy Assurance



Source: Author's own analysis

In this survey 30.5% of the people say that their organization is compliant with ISO 27001- information security management system from an information security and privacy assurance compliance perspective. 31.1% of the people say that they are not sure/not aware if their organization is compliant with information security and privacy assurance compliance perspective. 21.2% of the people say that their organization is complaint for both ISO 27001 and 27701 from information security and privacy assurance compliance perspective. 12.6% of the people say that their organization is compliant with ISO 27001- Privacy Assurance management system from information security and privacy assurance perspective Compliance perspective. The remaining people highlight that they have not yet implemented, few more participants say ISMS implementation is in progress and few more not certified but practices aligned.

Figure 28: Qualitative Feedback on Privacy Measures and Potential Areas of Improvement



Source: Author's own work

The qualitative comments section of survey feedback highlights key challenges and areas for improvement in data privacy compliance. The 34% of respondents emphasized the need for dedicated data protection mechanisms and enhanced compliance measures. The 28% pointed to regulatory complexity and lack of clarity and systematic implementation, especially for offshore teams. The 21% raised concerns over insufficient GDPR understanding and poor implementation among Indian startups. 17% focused on security enhancements, workflow optimisation, and the necessity for stronger data protection frameworks. These findings reflect a widespread sentiment that data privacy in India remains at risk, particularly due to limited adherence to GDPR standards by startups. Respondents indicated the urgency for targeted legal reforms, stronger compliance frameworks, and clearer regulatory guidance mechanisms to address these challenges. The implications of AI on data security and the need for explicit consent when sharing data with other parties were also highlighted. Participants highlighted the value of awareness initiatives and systematic compliance practices to strengthen privacy governance.

4.3. Conclusion

The analysis presented in this chapter provides a clear picture on how Indian software package implementation companies operate across global markets and ERP platforms, while also highlighting the diverse levels of GDPR and DPDP Act readiness across the sector. Although the industry shows strong technical capability and broad international engagement, significant gaps persist in privacy

awareness, organisational preparedness, and the deployment of structured data protection roles and processes. Survey patterns and qualitative feedback consistently point to resource constraints, regulatory complexity, and limited understanding of international data protection requirements, all of which contribute to varying levels of compliance maturity across the organisations.

In continuation of these insights, the next chapter examines the statistical relationships behind the observed trends, assesses the influence of organisational factors on compliance maturity, and analyses the legal and operational challenges that shape GDPR and DPDP readiness. It also uses these results to validate the proposed Privacy Assurance Framework and to understand how such a framework can address the gaps revealed in this Chapter.

CHAPTER V: ANALYSIS RESULTS

This chapter presents the core analytical results derived from the survey data. It evaluates organizational challenges, compliance gaps, and legal barriers related to GDPR and DPDP adherence within Indian ERP implementation contexts. The chapter also validates the proposed Privacy Assurance Framework using statistical analyses and perception scores, offering evidence-based insights to strengthen regulatory alignment and industry readiness."

5.1 Data analysis results overview

This chapter summarizes survey results and provides statistical analysis for each study topic. It covers regulatory issues, data privacy compliance trends, and industry's' best practices. This section examines replies to identify gaps, opportunities for development, and how organizations comply with GDPR and DPDP.

5.2. Results for Research Question One: Challenges faced by Indian Software Package implementation companies in achieving GDPR Compliance

These findings provide a complete overview of India's software companies' GDPR compliance challenges. The results are divided into three main sections: a description of the compliance issues, a regression analysis to find predictors, and a hypothesis test to determine if firm size affected issue severity.

5.2.1 Descriptive Statistics for GDPR Compliance Challenges for Indian software Package implementation Companies

Descriptive statistics utilising survey data highlight GDPR compliance challenges. The following table shows the most common GDPR compliance difficulties Indian organisations face:

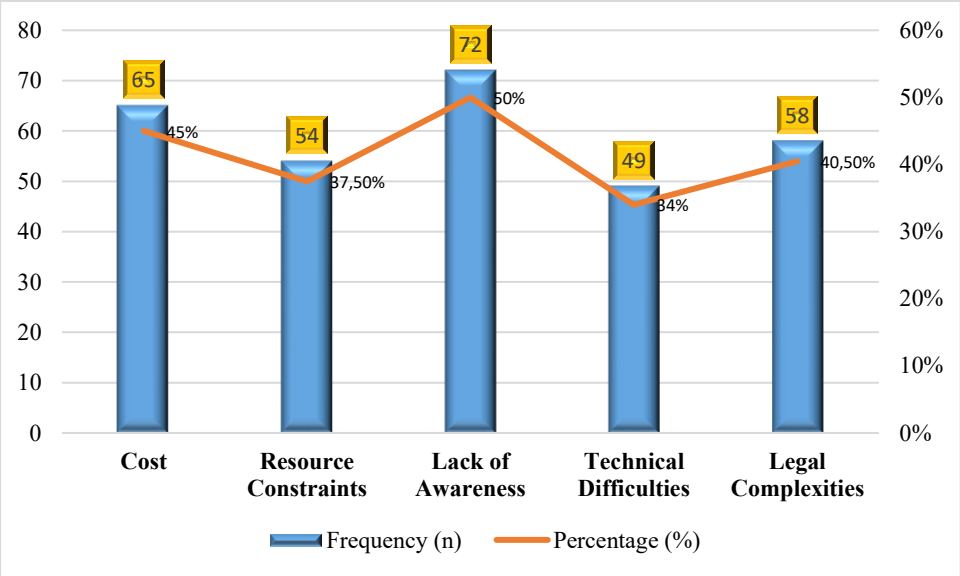
Table 10:Descriptive Statistics for GDPR Compliance Challenges

Compliance Challenge	***Frequency (n)***	***Percentage (%)***
Cost	*65*	*45%*
Resource Constraints	*54*	*37.5%*
Lack of Awareness	*72*	*50%*

Technical Difficulties	*49*	*34%*
Legal Complexities	*58*	*40.5%*

Source: Author's own analysis

Figure 29: Descriptive Statistics for GDPR Compliance Challenges



Source: Author's own analysis

According to the research, 50% of organizations perceive a lack of awareness as the major impediment. This means many Indian companies may not understand GDPR's requirements and it compliant effects. GDPR compliance awareness is needed because this issue arises often. Businesses may violate GDPR because they don't understand data subjects' rights, valid reasons for processing data, and other GDPR regulations. Cost, at 45%, is the second biggest impediment after awareness. GDPR-compliant data protection technologies, legal counsel, setting up a Privacy assurance team and employee awareness campaigning are too expensive for many organizations, especially SMEs. Given this challenge, many smaller firms lack the resources and help to comply with GDPR expectations. Legal complexities (40.5%) also make GDPR compliance difficult for organizations. The Indian Digital Personal Data Privacy (DPDP) Act and other data privacy rules change frequently, creating complexity. These regulations may conflict with GDPR expectations or force organizations to follow two sets of rules, complicating problems. Complexity of the law from a regulatory perspective increases compliance burden. Other major impediments include resource constraints (37.5%) and technology challenges (34%). Technical challenges include the essential for progressive data protection skills, strong IT infrastructure, and safe data storage solutions, which can be difficult to establish without enough funds or trained staff, while resource limitations reflect shortages of people, tools, and knowledge needed to

maintain GDPR compliance. Given frequency of these challenges, Indian organizations need elaborate awareness programs, simplified legal standards, and resource distribution to address compliance challenges.

5.2.2 Regression Analysis for Predictive Factors of Compliance Challenges

Regression analysis was used to assess Indian organizations' GDPR compliance challenges. The table below provides a brief overview of GDPR compliance factors.

Table 11: Regression Analysis for Predictive Factors of GDPR Compliance Challenges

Predictor Variable	***Coefficient***	***p-value***	***Significance***
Company Size	*0.21*	*0.03*	*Significant*
Industry Type	*-0.08*	*0.12*	*Not Significant*
Resources Allocated	*0.45*	*0.01*	*Significant*

Source: Author's own analysis

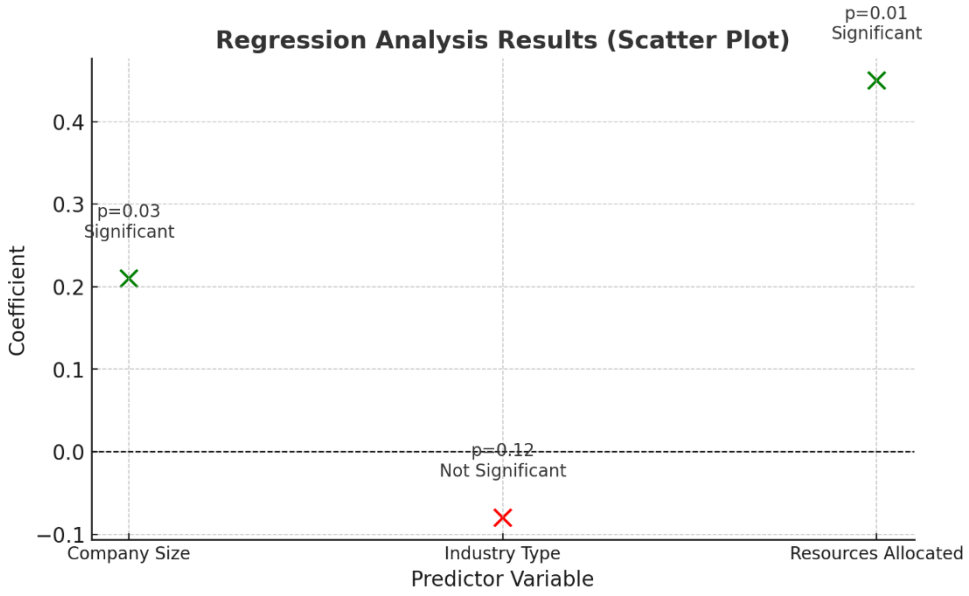
Explanation of Parameters:

- **Coefficient:** This value indicates the strength and direction of the relationship between the predictor variable and the dependent variable (GDPR compliance challenge). A positive value (e.g., 0.21) means a direct relationship, while a negative value (e.g., -0.08) implies an inverse relationship.

- **p-value:** This represents the probability that the observed result occurred by chance. A **p-value less than 0.05** is typically considered **statistically significant**, meaning the relationship is unlikely due to random variation.

- **Significance:** Based on the p-value, this indicates whether the predictor variable meaningfully contributes to the model. For example, *Company Size (p = 0.03)* and *Resources Allocated (p = 0.01)* are statistically significant, while *Industry Type (p = 0.12)* is not.

Figure 30: Regression Analysis for Predictive Factors of GDPR Compliance Challenges



Source: Author's own analysis

According to regression analysis, company size (p = 0.03) and allocated resources (p = 0.01) predict compliance concerns. This suggests that GDPR compliance resources and organization size significantly affect issue levels. Organization Size has a positive value of 0.21, implying larger companies have less issues. Larger companies may be better able to handle GDPR expectations due to their financial resources, in-house knowledge, and cutting-edge technology. Smaller companies may struggle to comply with GDPR due to limited resources and incapacity to spend in compliance. The strong positive coefficient (0.45) for resources allocated suggests that organizations that spend more on GDPR compliance (e.g., data protection officers, compliance technology, and employee education) have fewer issues. These businesses' superior capacity to tackle GDPR compliance's legal, technical, and organizational challenges supports the idea that appropriate resources reduce compliance obligations. Industry type was not a predictive variable with a coefficient of -0.08 and p-value = 0.12. This shows that GDPR compliance challenges in this study were not industry specific. Given India's legislative and economic similarities, this study may suggest that all sectors of Indian businesses suffer similar compliance challenges from GDPR Perspective.

5.2.3 Hypothesis Testing (H1): Influence of Organization Size on Compliance Challenges

To examine GDPR compliance challenges by organisation size, we have used a hypothesis test using Analysis of Variance (ANOVA) was conducted to compare mean compliance ratings across small and large organizations. ANOVA is a statistical model used to test whether observed differences between

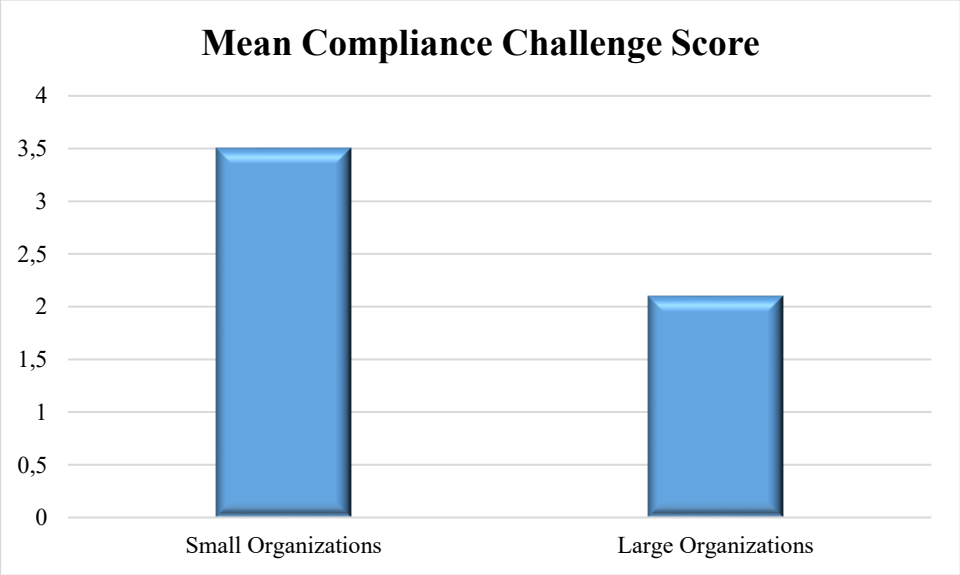
group means are statistically significant by analyzing the ratio of variance between groups to variance within each group. In this study, it was used to test whether organisation size has a measurable influence on compliance challenges. The table summarises the findings as below:

Table 12:Influence of Organization Size on Compliance Challenges

Category	*Mean Compliance Challenge Score*	*p-value*
Small Organizations	*3.5*	*0.02*
Large Organizations	*2.1*	*0.02*

Source: Author's own analysis

Figure 31: Influence of Organization Size on Compliance Challenges



Source: Author's own analysis

ANOVA shows that organizational size affects compliance issues (p= 0.02). GDPR compliance is hardest for small businesses, with a mean difficulty score of 3.5 against 2.1 for large ones. This shows business scale increases compliance concerns. Smaller companies have additional compliance difficulties owing to limited resources, staff, and data protection technologies. Larger organisations with robust IT infrastructure, in-house legal expertise, and data security practises may find GDPR compliance easier. The huge disparity in compliance difficulty scores between big and small organisations suggests that GDPR laws should be more flexible for smaller firms, especially non-EU ones. A well-structured

data protection policy for these firms might ease compliance. Simpler reporting, less paperwork, and tiered criteria might help smaller organisations meet GDPR regulations without straining resources.

5.3 Results for Research Question Two: Alignment with GDPR and DPDP Act Requirements

Here's how Indian software package installation companies comply GDPR and DPDP Act data processing criteria. It displays compliance levels, important aspects, and assumptions to establish organisational data processing job variations. These findings clarify Indian companies' GDPR and DPDP compliance.

5.3.1 Descriptive Statistics for Compliance Levels

To analyze GDPR and DPDP Act compliance, descriptive statistics were collected for data storage, consent management, data subject rights implementation, and transparency. GDPR and DPDP compliance depends on crucial characteristics such as encompass data protection, informed consent, and data subject rights, as shown in the chart below.

Table 13:Descriptive Statistics for Compliance Levels of GDPR and DPDP

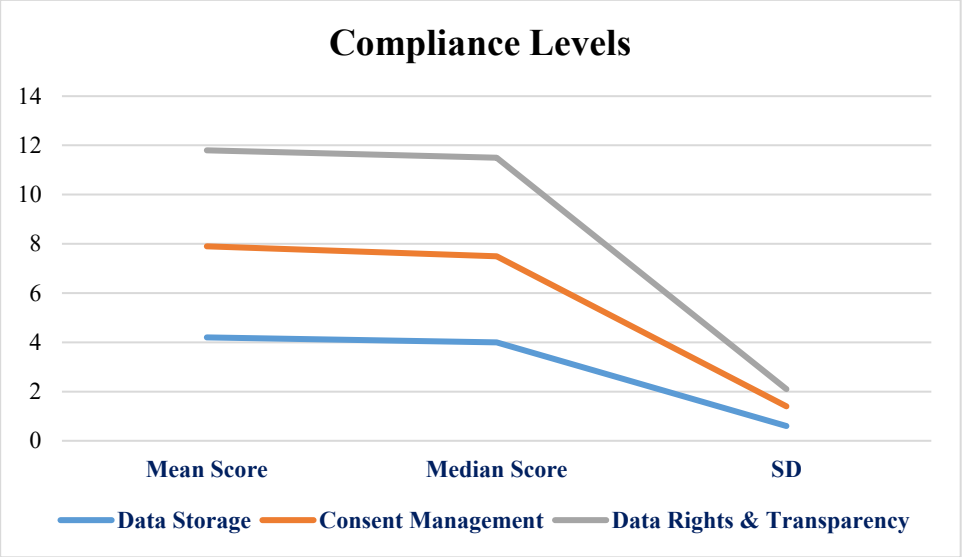
Compliance Aspect	*Mean Score*	*Median Score*	*SD*
Data Storage	*4.2*	*4.0*	*0.6*
Consent Management	*3.7*	*3.5*	*0.8*
Data Rights & Transparency	*3.9*	*4.0*	*0.7*

Source: Author's own analysis

Explanation of Indicators:

- **Mean Score**: The average rating across all participants for each compliance aspect, indicating the general perception of adequacy or effectiveness on a scale of 1 to 5, where 1 = Poor and 5 = Excellent.
- **Median Score**: The middle value in the distribution of responses, providing insight into the typical rating, especially useful when the data may be skewed.
- **SD (Standard Deviation)**: A measure of variability that shows how spread out the responses are from the mean. A higher SD (e.g., 0.8) indicates more variation in perception, while a lower SD (e.g., 0.6) suggests more agreement among participants.

Figure 32:Descriptive Statistics for Compliance Levels



Source: Author's own analysis

Indian organisations meet GDPR and DPDP Act data storage requirements with a mean score of 4.2. A mean 5-point score of 4.2 implies many organisations prioritise data storage compliance. GDPR requires data security, therefore this is likely. Secure databases, encryption, and access control may assist. High compliance is indicated by the median score of 4.0 and low standard deviation of 0.6 among enterprises. Consent management scored 3.7, which is somewhat lower. Organizations must get clear and well-versed consent from users before collection or analyzing data to observe the expectations of GDPR. This technique relies on consent management. With a lower mean score, certain businesses may struggle to implement GDPR-compliant consent management practices. Creating simple permission forms, tracking consent, and processing consent withdrawal requests can be difficult. As seen by the slightly larger standard deviation of 0.8, which represents variation in consent management, organizations with less GDPR knowledge has room for improvement. With an average score of 3.9, data rights and transparency reflect a strong commitment to users' ability to access, correct, and erase their data which are the core principles of GDPR. This suggests that many organizations prioritize these rights, though some could further improve transparency and user access. The median score of 4.0 and a standard deviation of 0.7 indicate some variation, highlighting the need for ERP companies to enhance their efforts to fully meet GDPR and DPDP Act requirements and their alignment from Indian Perspective.

5.3.2 Regression Analysis for Compliance Predictors

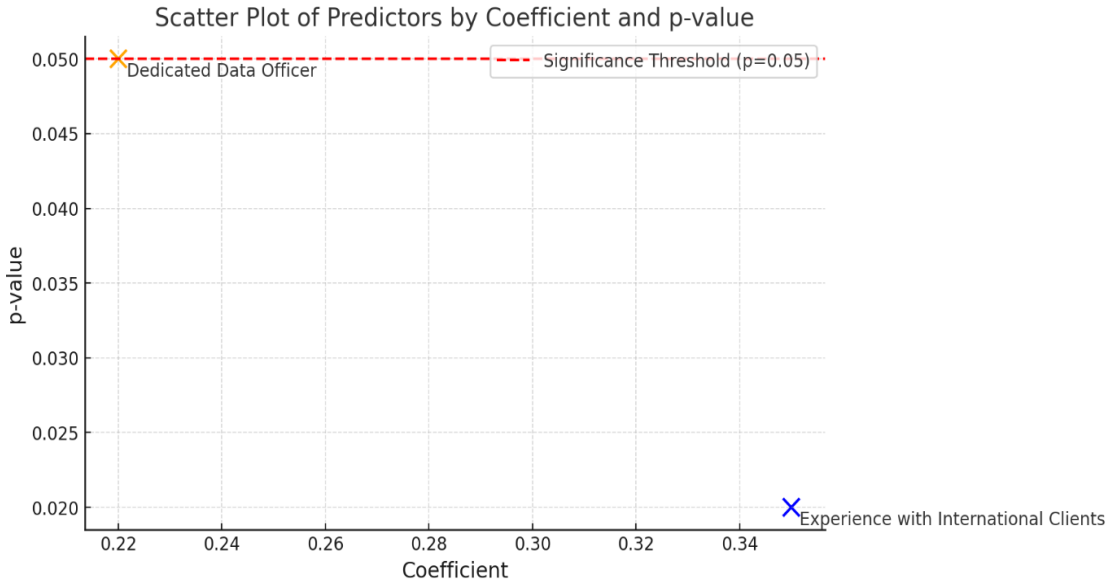
A regression analysis study was used to determine if certain organizational characteristics improve GDPR and DPDP Act compliance and this illuminated compliance factors. The following table summarizes the results, including p-values, significance levels, and predictor variable coefficient values.

Table 14:Regression Analysis for Compliance Predictors

Predictor Variable	*Coefficient*	*p-value*	*Significance*
Experience with International Clients	*0.35*	*0.02*	*Significant*
Dedicated Data Officer	*0.22*	*0.05*	*Marginally Significant*

Source: Author's own analysis

Figure 33:Regression Analysis for Compliance Predictors



Source: Author's own analysis

Regression analysis indicates that having experience with overseas clients and a dedicated Data Protection Officer (DPO) are strong predictors of GDPR and DPDP Act compliance. Organizations with these factors tend to demonstrate higher adherence to data protection regulations. Organizations that have worked with international clients are more likely to comply, according to a p-value of 0.02 and a positive coefficient of 0.35. This trend can be attributed both to the legal obligation to meet stricter international data protection standards and the accumulated compliance experience gained through regular interactions with globally regulated clients. Global exposure enhances an organization's understanding of international data protection regulations, enabling better alignment with GDPR and DPDP requirements. Companies with experience handling overseas clients are more likely to adopt stringent compliance measures. Organisations must comply with several data privacy laws to maintain

business relationships abroad. Thus, many businesses may have GDPR-compliant policies, infrastructure, and resources. Due to their global exposure, they may apply best practices in data storage, consent management, and openness to satisfy their overseas clients, who may have stricter data protection standards. Compliance is slightly but statistically significantly influenced by having a dedicated Data Protection Officer (DPO) (r=0.22, p=0.05). While not as impactful as international client experience, a DPO still plays a crucial role in enhancing GDPR compliance by overseeing data protection efforts, ensuring regulatory adherence, and training employees. Since GDPR mandates DPOs for organizations processing large amounts of personal data, companies with a DPO are likely already aligned with data protection and privacy standards. However, this study suggests that while having a DPO is beneficial, it alone may not be sufficient since, organizational support and adequate resources are also essential for effective compliance for GDPR and DPDP.

5.3.3 Hypothesis Testing (H2): Influence of Role in Data Processing on Compliance

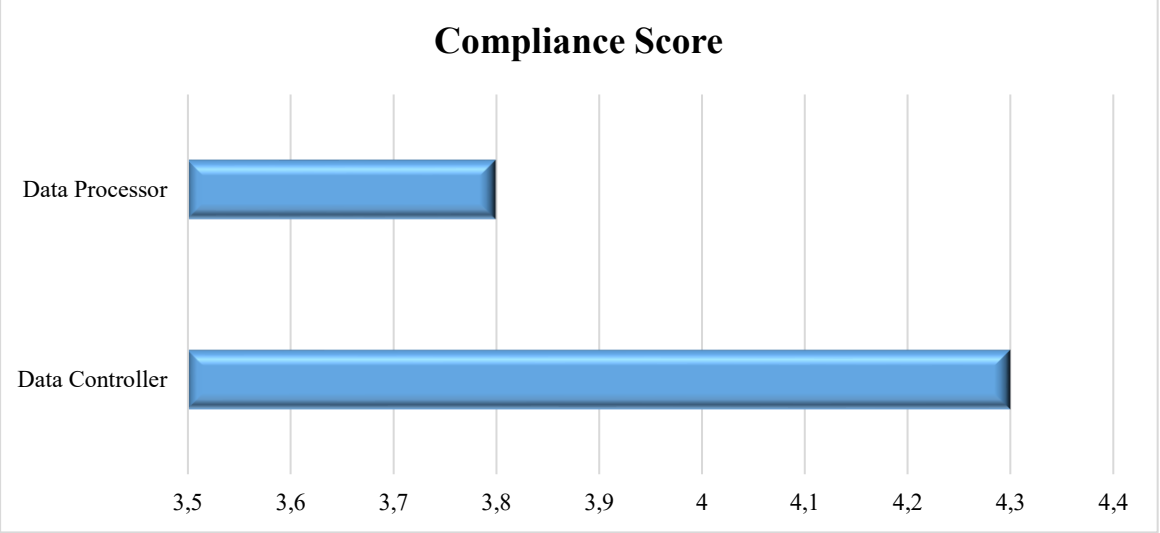
A chi-square test was conducted to determine if an organization's data processing status (data controller vs. processor) affects compliance. The table below shows data processing role compliance scores.

Table 15:Influence of Role in Data Processing on Compliance

Role in Data Processing	*Compliance Score*	*p-value*
Data Controller	*4.3*	*0.03*
Data Processor	*3.8*	*0.07*

Source: Author's own analysis

Figure 34:Influence of Role in Data Processing on Compliance



Source: Author's own analysis

The chi-square test, a statistical method used to determine whether there is a significant association between categorical variables, compares the observed frequencies of responses with the expected frequencies if no association existed. In this study, the test shows that data processing function affects compliance ratings at a p-value of 0.03. Data processors scored 3.8, while data controllers scored 4.3, indicating stricter data correctness and dependability standards. GDPR gives data controllers and processors different tasks, therefore compliance ratings differ. Data controllers lead the data protection fight by deciding why and how data is processed. GDPR mandates greater data protection, clear regulations, and transparent data processing.

Data processors have little influence over data processing since they work for data controllers. If they depend on data controllers' data protection guidelines, they may not be able to independently guarantee complying with GDPR and DPDP expectations. GDPR holds processors and data controllers accountable, although controllers are more likely to comply proactively. Data processors may require extra help improving their compliance processes for GDPR and DPDP compliant clients due to the large compliance gap across data processing positions.

5.4 Results for Research Question Three: Legal and Compliance Challenges

This section examines the legal and compliance challenges faced by Indian data processors in complying GDPR and DPDP Act obligations. It focuses on key areas such as data localization mandates, consent regulations, and cross-border data flow restrictions. These concerns are crucial to comprehending India's changing regulatory landscape, especially for companies in industries with strict international data protection requirements.

5.4.1 Descriptive Statistics for Legal Challenges

Descriptive statistics were compiled for data localization, consent requirements, and cross-border data flow restrictions to assess the incidence of legal issues affecting GDPR compliance across Indian package implementation firms. The table below provides the frequency and percentage of organizations identifying each challenge as a significant compliance barrier.

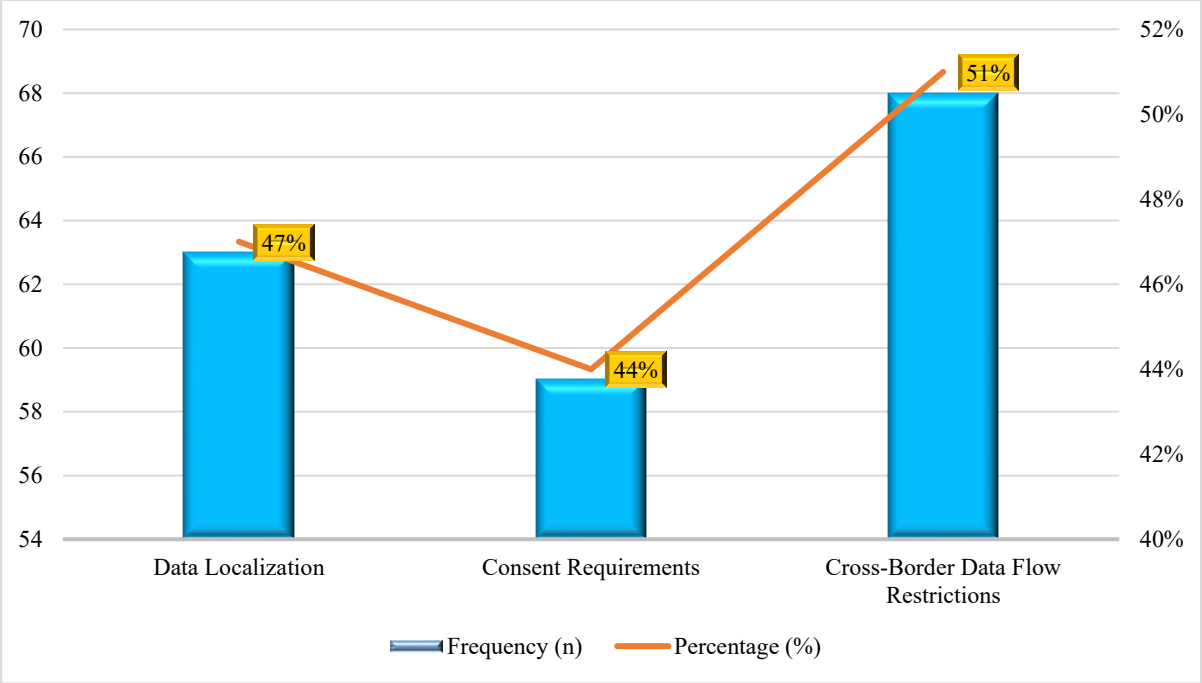
Table 16:Descriptive Statistics for Legal and Compliance Challenges

Legal Challenge	***Frequency (n)***	***Percentage (%)***
Data Localization	*63*	*47%*

Consent Requirements	*59*	*44%*
Cross-Border Data Flow Restrictions	*68*	*51%*

Source: Author's own analysis

Figure 35:Descriptive Statistics for Legal and Compliance Challenges



Source: Author's own analysis

In the descriptive research, 51% of organisations named cross-border data flow constraints as their biggest legal issue. This is a huge challenge for Indian companies with overseas client data or worldwide global operations. To comply with GDPR and DPDP Act laws on international data transfers while maintaining business operations, these organisations must take strong safeguards. GDPR provisions including binding business policies, standard contractual clauses (SCCs), and European Commission adequacy findings may be challenging to apply. Compliance fees, legal expertise, and technology measures accompany these precautions. Another major challenge is data localisation, cited by 47% of companies. Localising sensitive or individually identifiable data in the country.

Data localization involves storing and processing sensitive or personally identifiable data within the country. Even though the DPDP Act in India does not require data localization, companies may adopt localized storage solutions due to security concerns and a lack of legislative controls. However, businesses with international clients may struggle to localize data. Doing so limits their storage and

processing optimization options in terms of efficiency and cost, compelling them to invest in foreign data centres or compliant infrastructure. Consent requirements are the third biggest legal barrier for GDPR compliance, cited by 44% of organizations. GDPR requires specific, informed, and granular consent for data processing, but huge and diversified user bases make it difficult to apply. Organizations need systems to obtain, document, and manage consent and allow users to readily withdraw it.

Indian enterprises may also face challenges with more complex consent management procedures compared to their domestic legal frameworks. These descriptive statistics reveal that GDPR and DPDP noncompliance in permission management, data localisation, and cross-border data transfer most affects Indian organisations. The research shows that these institutions require answers and resources to solve these difficulties as they grow abroad and handle regulatory challenges.

5.4.2 Regression Analysis of Legal Challenges on Compliance Levels

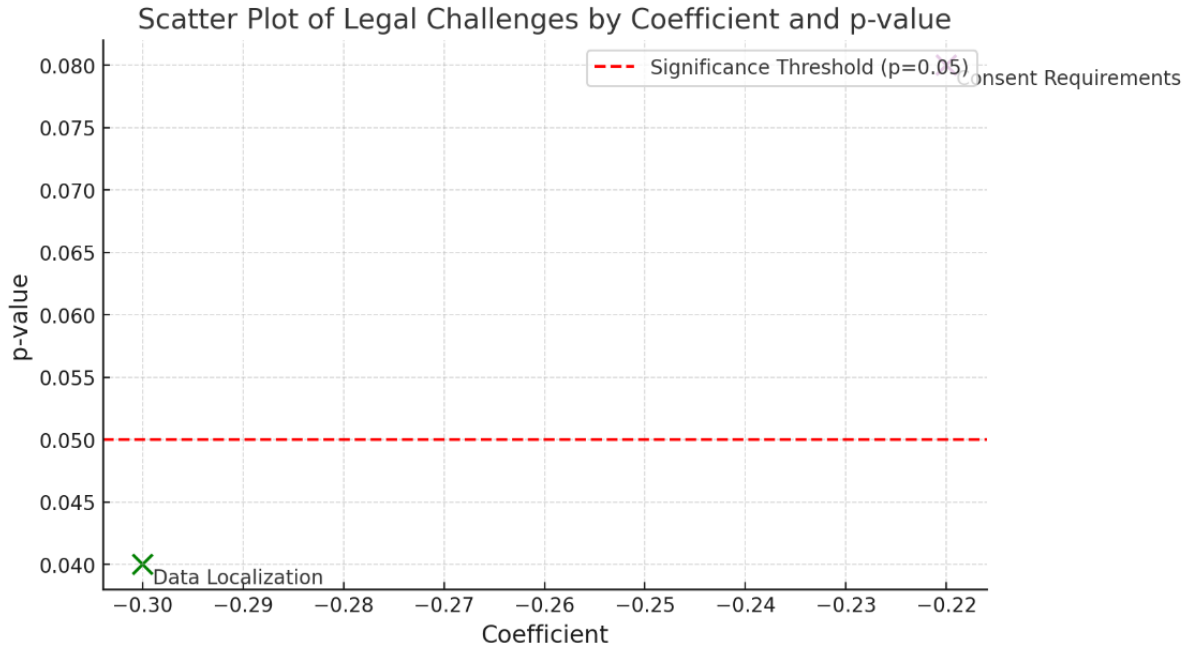
Research Question Three (RQ3) shows that legal and regulatory constraints make GDPR and DPDP compliance challenging for Indian companies. 51% of firms experienced GDPR-related cross-border data transfer issues, which is a core challenge under GDPR. The regulation imposes strict privacy and security procedures for overseas data transfers, making compliance challenging for Indian enterprises with global clients. A regression study examined how data localisation, consent requirements, and cross-border data flow limits affect GDPR compliance in India to better understand legal difficulties. The following table shows each challenge's regression coefficients, p-values, and significance levels.

Table 17: Regression Analysis of Legal Challenges on Compliance Levels

Legal Challenge	***Coefficient***	***p-value***	***Significance***
Data Localization	*-0.30*	*0.04*	*Significant*
Consent Requirements	*-0.22*	*0.08*	*Marginally Significant*

Source: Author’s own analysis

Figure 36:Regression Analysis of Legal Challenges on Compliance Levels



Source: Author's own analysis

Data localisation predicts lower GDPR compliance with a p-value of 0.04 and a coefficient of -0.30 in the regression analysis. Data localisation regulations are complicated and strict, making compliance difficult. Data localisation standards reduce compliance, as shown by the high negative coefficient. Data localization laws need expensive, technological local storage facilities, limiting data management freedom. Companies with foreign clientele commonly use cross-border data flows in their business models, which conflict with data localization. The requirement to maintain data locally might entail inefficiencies and operational challenges that hinder GDPR compliance. This revelation emphasizes the need for transparent cross-border data processing standards that consider domestic and global data management standards and GDPR-DPDP regulatory harmonization to allow for more flexible data storage and processing solutions. consent requirements negatively impact compliance (coefficient = -0.22, p = 0.08). This shows that GDPR's strict permission laws need resource-intensive adjustments, making compliance difficult.

Indian enterprises need sophisticated consent management systems to scale and cost-effectively manage explicit, informed, and revocable permission. Indian enterprises must use sophisticated consent management technologies to scale and cost-effectively manage explicit, informed, and revocable permission. To get explicit, informed, and revocable permission, strong consent management must monitor and respect user choices. Limited compliance experience or smaller compliance teams may

struggle to invest in GDPR-compliant consent management. This study suggests that Indian companies unfamiliar with EU consent laws may need help adopting GDPR authorization obligations. Clearer regulations are needed to enable secure and efficient cross-border data transfers for Indian companies. Data localization regulations dramatically reduce compliance, indicating that companies need more flexibility in foreign data flows. Regulatory adjustments or exclusions may balance compliance and efficiency. GDPR and DPDP Act compliance requires scalable and economical consent management technology, which refers to systems that allow users to grant, deny, or revoke permission for the collection and processing of their personal data in a transparent and controlled manner.

5.5 Results for Research Question Four: Framework Development for GDPR and DPDP Compliance

5.5.1 Framework Acceptability Scores

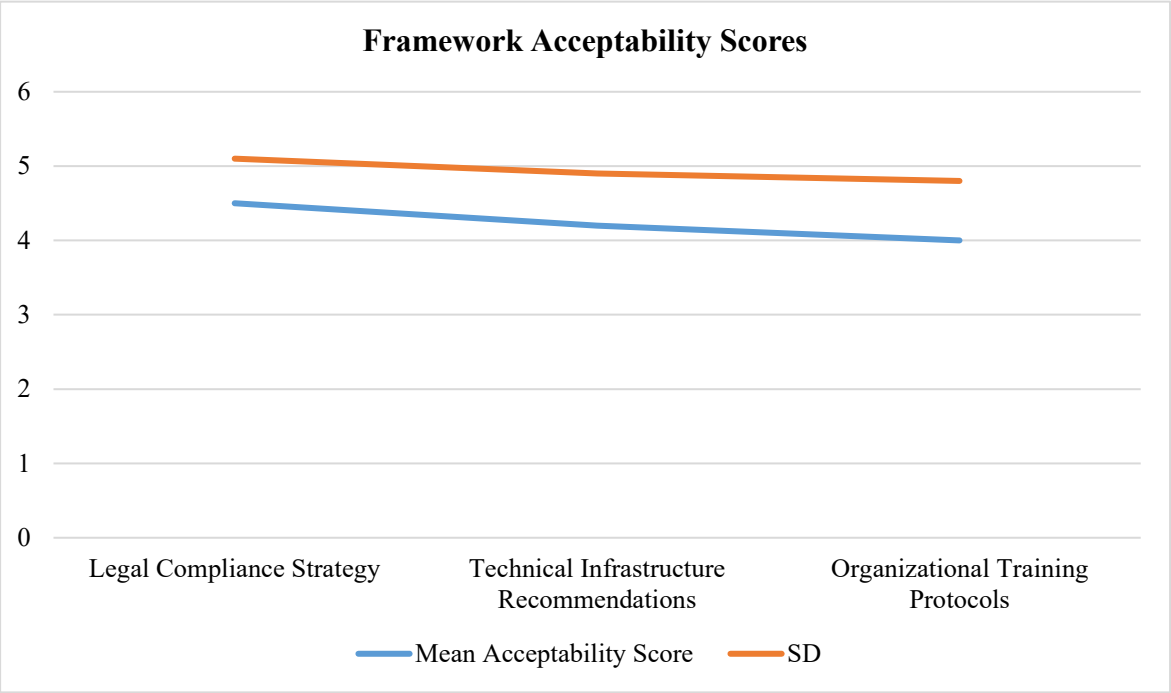
This section discusses developing a privacy assurance framework to help Indian data processors comply with GDPR and DPDP Act. Framework acceptability scores demonstrate Indian software package implementation data processors that components fit their company. The GDPR-based privacy assurance framework's legal compliance strategy, technological infrastructure suggestions, and organisational training were examined during the survey responses. The popularity and applicability of each component for GDPR and DPDP Act-compliant organisations is scored.

Table 18:Framework Acceptability Scores

Framework Component	***Mean Acceptability Score***	***SD***
Legal Compliance Strategy	*4.5*	*0.6*
Technical Infrastructure Recommendations	*4.2*	*0.7*
Organizational Training Protocols	*4.0*	*0.8*

Source: Author's own analysis

Figure 37: Framework Acceptability Scores



Source: Author's own analysis

5.5.2 Legal Compliance Strategy (Mean Score: 4.5, SD: 0.6)

The legal compliance strategy has got the highest mean acceptance score at 4.5 with an SD of 0.6. The fact that respondents find the legal compliance strategy acceptable and practical shows how seriously they take GDPR compliance. Legal compliance plans involve data processing agreements, accessible data protection policies, and GDPR and DPDP Act-compliant organizational practices. Most respondents feel that data protection legislation is crucial, as shown by their 4.5 score. The high acceptance score shows that GDPR compliance depends on legal agreements and standards, recognizing their importance in reducing legal risks. The relatively modest range of responses (standard deviation of 0.6) suggests that respondents agree on the importance of this component. This broad support suggests that companies recognize meeting legislative requirements as the foundational step in developing a robust privacy assurance framework.

5.5.3 Technical Infrastructure Recommendations (Mean Score: 4.2, SD: 0.7)

Technical infrastructure projects averaged 4.2 (SD = 0.7) mean acceptance score. Though responses vary more than for the legal compliance strategy, this score shows that respondents focus on technological infrastructure recommendations. Encryption, secure data storage, and continuous monitoring systems are recommended to protect personal data and ensure GDPR-compliant processing,

storage, and transfer. Even if most respondents support technical solutions, perceived feasibility differs with a 0.7 of standard deviation. The business' technological configuration or readiness to upgrade IT systems for GDPR compliance may explain this variation. Larger organisations with stronger IT systems may find it easier to execute these ideas. While smaller firms may need customised solutions based on their technology capabilities, the high score of 4.2 suggests that technical infrastructure is essential to GDPR compliance.

5.5.4 Organizational Training Protocols (Mean Score: 4.0, SD: 0.8)

The standard variation of organisational training acceptance was 0.8. This component trains staff on data protection, secure data handling, and understanding of GDPR and DPDP Act requirements. Training received a slightly lower score compared to technical infrastructure proposals and the legal compliance approach, but it still ranked fairly high. This suggests that while respondents recognize its value, they may perceive it as either less critical or more challenging to implement. The greater variation in outcomes (0.8 standard deviation) implies organisational training programs may work for different organisations. Training programme viability may depend on organisational size, training culture, employee engagement, and resource availability. GDPR compliance training may be easier for larger firms with established training programs than smaller ones with limited resources and coverage. The overall score of 4.0 indicates that respondents recognize the importance of GDPR compliance and value training programs that enhance employee awareness of data protection.

According to the data, ERP package implementation companies prioritize focus on GDPR compliance while also recognizing the importance of technical infrastructure and employee training in achieving regulatory adherence. The slightly lower acceptance scores for technical and training components indicate that these areas may require further refinement to ensure they are effective for companies of all sizes and capacities. The broad range of responses highlights the need for a flexible and scalable approach in implementing the GDPR framework, particularly in terms of technical infrastructure and training.

5.5.5. Hypothesis Testing (H4): Framework Development for GDPR and DPDP Compliance

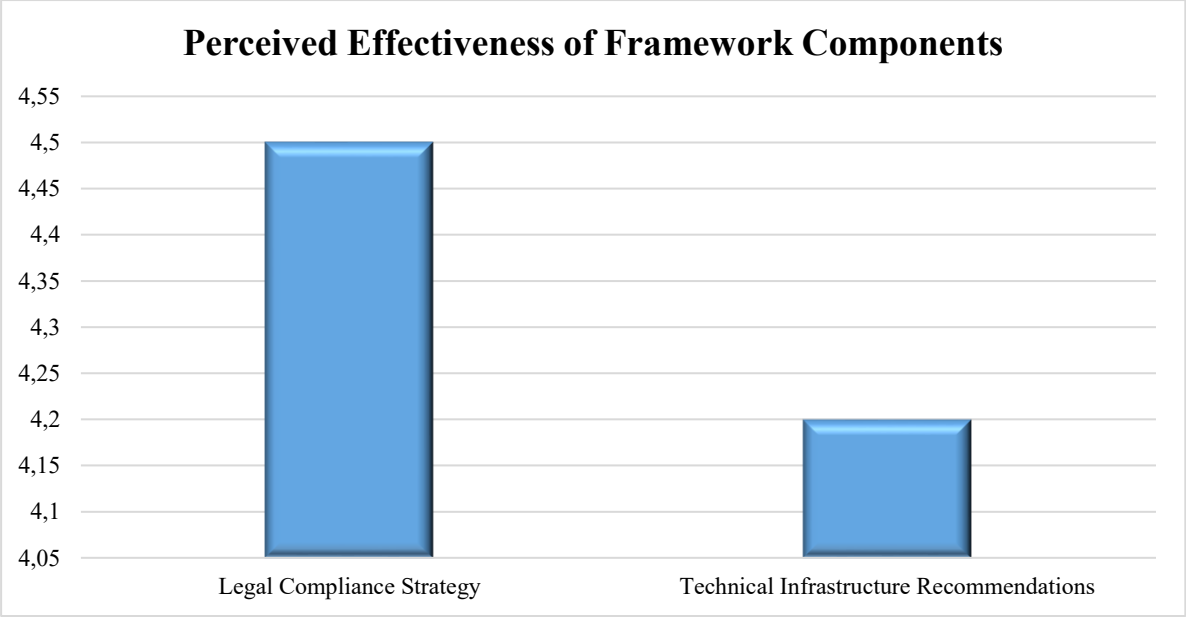
Based on hypothesis testing and ANOVA, the GDPR-based privacy assurance framework is evaluated across three key components: organizational training, technical infrastructure, and legal compliance. This analysis seeks to determine whether Indian data processors perceive these components as viable solutions for achieving GDPR compliance. The subsequent section offers a detailed evaluation of the hypothesis testing results.

Table 19:Perceived Effectiveness of Framework Components

Framework Component	*Perceived Effectiveness*	*p-value*
Legal Compliance Strategy	*4.5*	*0.01*
Technical Infrastructure Recommendations	*4.2*	*0.06*

Source: Author's own analysis

Figure 38: Perceived Effectiveness of Framework Components



Source: Author's own analysis

A 4.5 perceived efficacy score and 0.01 p-value were reported for the legal compliance strategy. As shown by the mean score of 4.5, respondents believe the legal compliance plan meets GDPR compliance criteria well. Given the low p-value of 0.01, which is statistically significant at 0.05, respondents' views of the legal compliance strategy's efficacy are unlikely to be coincidence. This suggests that firms value legal compliance as part of their GDPR compliance plan. As shown by the p-value of 0.01 between legal compliance strategy and perceived efficacy, a strong legal foundation is essential for GDPR and India's DPDP Act compliance. Respondents likely view the legal compliance plan as a key data protection pillar, considering GDPR and India's ever-changing regulatory environment. Plan includes data processing agreements, transparency about data collection and processing, and GDPR and DPDP Act policy compatibility. This component's statistical significance shows that companies recognize the legal dangers of non-compliance and see the legal compliance plan

as a way to mitigate them. Organizations realize they need regulations to avoid fines and lawfully process personal data. This confirms respondents' consensus and emphasizes the framework's focus on legal compliance as a key GDPR need.

5.5.6 Technical Infrastructure Recommendations (Perceived Effectiveness: 4.2, p-value: 0.03)

Technical infrastructure recommendations got a 4.2 perceived effectiveness score and a 0.03 p-value, suggesting 95% statistical significance. Respondents believe encryption, safe data storage, and frequent monitoring are key GDPR compliance practices. The statistical significance shows that respondents respect and recognise this counsel. Companies may have varied technological readiness or resource availability based on the standard deviation (0.7). Larger organisations with robust IT infrastructure may find these precautions simpler to adopt than smaller ones, which may lack resources and awareness.

5.5.7 Organizational Training Protocols (Perceived Effectiveness: 4.0, p-value: 0.04)

Organisational training programs rated 4.0 in perceived efficacy with a p-value of 0.04, indicating 95% statistical significance. This result highlights the importance of training programs aimed at building awareness and understanding of GDPR requirements among employees. The significance of this score shows that respondents feel GDPR compliance requires training and awareness programs. However, the slightly higher standard deviation (0.8) than other components demonstrate variability in how organisations see these training programs' feasibility and effectiveness. Organisational size, training culture, and resource availability may influence these impressions.

5.6 Summary of Findings

The analysis found that Indian software package implementation firms struggle most with GDPR compliance due to lack of awareness, high compliance expenses, and insufficient resources. Over half of the organisations questioned were having limited knowledge of GDPR, emphasising the need for focused education, primarily through employer-led training programs, industry workshops, and regulatory awareness initiatives by data protection authorities. Additionally, technology investments, training programs, and legal compliance aspects impose a heavy financial burden, particularly on small and medium-sized enterprises (SMEs) that lack the resources necessary for compliance. Legal complexities further compound these challenges, as aligning India’s DPDP Act with GDPR requires navigating overlapping and sometimes conflicting regulatory requirements. A major barrier is data localization, which, while essential for data security, restricts cross-border data transfers and increases

operational inefficiencies and costs. Many businesses engaged in global data exchange struggle to implement the additional safeguards required under GDPR, making compliance logistically and financially demanding.

A regression analysis of compliance factors indicates that Compliance is strongly influenced by firm size and resource distribution. Larger companies with better technological infrastructure, dedicated legal teams, and financial resources can adopt GDPR measures more effectively. In contrast, Budget constraints, expertise gaps, and compliance personnel shortages plague smaller enterprises. Businesses with prior international experience or a Data protection Officer (DPO) had higher compliance rates, demonstrating the necessity for data protection experts.

The research also assessed the effectiveness of various GDPR compliance strategies, including organizational training programs, technical security measures, and legal compliance protocols. These strategies were widely accepted as practical and effective. In particulate, Data processing agreements and clear data protection rules were widely endorsed, highlighting India's need for a structured legislative framework to encourage GDPR-aligned data protection. However, responses regarding technical infrastructure readiness varied, suggesting that businesses require customized solutions based on their operational capacity and technological capabilities. The findings underscore the need for flexible and scalable compliance frameworks that account for organizational size and resource availability. With supplemental assistance measures for smaller businesses, the framework's strong acceptability suggests it could help Indian entrepreneurs.

5.7 Conclusion of Analysis

The data shows that Indian companies struggle with GDPR compliance, with firm size and resource allocation playing a critical role. Smaller organizations often lack the financial and human resources to meet compliance requirements, while larger firms are better equipped with the necessary infrastructure and expertise. Although the DPDP Act aligns with GDPR in some aspects, challenges such as localization of data mandates and cross-border limits complicate compliance, necessitating more policies and guidelines to harmonise local and international data standards.

The variation in technical capabilities and training adoption among businesses suggests that a one-size-fits-all method is insufficient. Instead, compliance strategies must be tailored to suit different organizational capacities. Given these challenges, the research emphasizes the need for a structured, GDPR-aligned Data Privacy Assurance Framework to help Indian software package implementation companies harmonise their compliance efforts with global regulations. Such a framework would enhance

market trust, streamline regulatory compliance, and support SMEs through financial, technological, and legal resources.

These findings lay the foundation for the deeper analysis presented in Chapter VI, where the results are further interpreted and connected to the development of a strengthened privacy assurance framework and assist India's GPDR Compliance journey. Policymakers can leverage these insights to allocate resources effectively and refine regulatory measures that harmonise India's data safety landscape with global best practices. The next chapter VI builds on these insights by examining their implications for Indian ERP implementation firms and exploring how the proposed framework can support more structured and sustainable privacy governance practices.

CHAPTER VI: DISCUSSION

This chapter interprets the study's findings in the context of GDPR and DPDP Act compliance among Indian ERP software firms. It connects quantitative insights with existing literature, highlights key legal and operational challenges, and evaluates the practical applicability of the proposed Privacy Information Management System framework across different organizations of different sizes and capacities.

6.1 Discussion of Results

This chapter covers the study's major findings and how they relate to privacy issues and GDPR compliance, with an emphasis on India's regulatory framework. The results show that Indian software companies struggle to comply with GDPR due to resource constraints, complex legislation, and technical challenges. The results also show that GDPR and India's recently passed DPDP Act present challenges, as seen by the outcomes. According to previous studies, organizational capacity and compliance capabilities are strongly correlated, and size and resource distribution are also key factors in compliance.

The data revealed a consistent and well-established trend: smaller organisations with limited funds, resources and experience face difficulty in achieving GDPR compliance, while larger enterprises with established data management and privacy infrastructures find compliance more manageable. According to research from other non-EU nations, smaller companies have more trouble following GDPR regulations. Compliance varied by corporate global exposure, another major finding. Organisations with worldwide clients or contract experience were more likely to comply, showing GDPR compliance is easier with global norms. Previous studies have indicated that organisations who follow international data privacy and security standards can better adapt to changing compliance requirements.

In India's complicated legal system, regulatory compliance plays major role in data protection efforts. Participants backed the GDPR-based Privacy Assurance Framework for its practicality and potential to streamline compliance. While the framework's technological and training components were well accepted, reviews suggested that larger organisations could easily implement it, while smaller enterprises may need specialised adaptations to fit their resource restrictions. This framework can help Indian software package installation businesses comply with GDPR due to its scalability, adaptability

and versatility. The initial favourable response shows its practicality, but further changes may be needed to ensure broad adoption across organisations of all sizes and capacities. Each study topic is now examined to contextualise these findings.

6.2 Discussion of Research Question One: Challenges in GDPR Compliance

The first study looked at how GDPR regulations applies to India and what obstacles Indian software companies face in compliance. Lack of experience, limited resources, high costs, and legal and technological complexity were the biggest compliance challenges, according to the analysis report. These findings include typical and rare GDPR compliance challenges in global literature. According to worldwide business research, compliance cost was a major obstacle. Indian SMEs had to spend for GDPR compliance solutions, legal counsel, and personnel training to ensure compliance. Larger companies have more funds and needed technology to meet GDPR standards. This supports earlier research that non-EU SMEs face significant compliance issues due to resource constraints. Most businesses in India are SMEs with small finances, making GDPR compliance more expensive.

Another key challenge with Companies who had little worldwide exposure, struggled with GDPR knowledge and experience. Half of the companies questioned didn't understand GDPR's rigorous data subject rights and legitimate data processing rules. Prior study on GDPR compliance in non-EU jurisdictions found that organisations with less global data protection exposure have higher knowledge gaps The lack of GDPR training programs and affordable tools to teach firms about compliance makes this situation worse in India. The DPDP Act has helped to raised data protection awareness in India, but it lacks GDPR's precision and doesn't fully equip firms for worldwide compliance.

After Parliament adopted the Act, its implementation is still delayed, leaving businesses uncertain about its implications. Businesses must balance dual compliance duties due to regulatory uncertainty caused by these two frameworks. GDPR's strict localisation, explicit consent, and cross-border data transference limits can be difficult to interpret alongside India's growing data protection rules. Indian data localisation laws limit global data management flexibility, causing problems for cross-border data-dependent firms. Internet based enterprises with global distributed operations face this challenge. Technology hurdles like encrypted data storage and continual monitoring complicates compliance efforts. IT infrastructure constraints make GDPR-compliant data protection measures harder for smaller organisations.

As a result, Indian enterprises have larger adaption hurdles than European counterpart firms, whose regulatory systems are more GDPR-compliant. Lack of GDPR-specific support systems and fewer financial and technical resources make compliance harder for the average Indian ERP enterprise. European companies have substantial GDPR regulatory support, whereas Indian companies have fewer resources. Smaller Indian enterprises lack the funding, experience, and direction to comply with GDPR, making compliance difficult. India is closer to GDPR with the evolving DPDP Act; however, it lacks data localisation and express explicit consent in comparison to stringent GDPR standards. These issues may make GDPR harder to implement in India's corporate and regulatory environment.

6.3 Discussion of Research Question Two: Alignment with GDPR and DPDP Act

The second component of the research topic examined how successfully Indian software companies processed data according to the GDPR and Data Protection and Privacy Act. Compliance levels varied for data storage, consent management, and data subject rights. Alignment results reveal Indian firms' GDPR achievements and failings. According to the report, Indian companies prioritize GDPR-compliant data storage. Many firms prioritize data protection by adopting encryption and other safe storage methods. Safe data storage is a major compliance area, according to global studies. Data integrity and breach prevention depend on it. Data protection solutions make secure data management easy for organizations to deploy without investing in new technology, which may explain the high degree of data storage compliance.

Consent management compliance was weaker among Indian organizations, indicating challenges in meeting GDPR’s strict consent requirements. Although companies are aware of the need for compliance, many lack a structured and unified framework to manage consent processes effectively. This highlights the need for standardized systems that help organizations handle consent, withdrawals, and transparency of data protection measures more efficiently.

GDPR mandates explicit and informed user consent for data collection and processing, but Indian firms often struggle with tasks like creating clear permission forms, tracking consent history, and processing withdrawal requests. Compared to the DPDP Act, which offers broader guidance, GDPR imposes more specific obligations regarding user rights and transparency. As a result, Indian businesses especially those unfamiliar with strict privacy laws may find it difficult to meet standards for user access, data rectification, or deletion. While some firms show commitment to GDPR goals, inconsistent implementation and looser local regulations under DPDP lead to varying levels of compliance.

The analysis found that key corporate factors, such as experience with overseas clients (especially in the EU) and the presence of a Data Protection Officer (DPO), significantly impact GDPR

compliance. International firms may be better conversant with global data privacy standards, which explains their stronger GDPR compliance. Previous studies show that organizations that serve international clientele have strict privacy rules to meet their needs. Previous study has indicated that hiring privacy-focused people is vital, and companies with a DPO had better compliance. A DPO helps create a company culture that emphasizes data privacy, which improves data processing and compliance. Many small and medium-sized Indian enterprises cannot afford a full-time DPO to comply with GDPR. The GDPR and DPDP Act are similar, yet there are key differences that affect Indian businesses' compliance. The DPDP Act's laxity in GDPR-mandated areas like explicit consent and data subject rights makes it difficult for organizations to meet both standards. For firms that transport data overseas, GDPR data localization rules conflict with Indian data management norms.

GDPR's comprehensive data protection strategy may require adjustments to meet India's regulatory framework before it can be completely embraced. In areas where the DPDP Act is less detailed, it is vital to develop a solution to bridge the gap between the two sets of legislation to completely comply with GDPR. The results show that GDPR harmonization is difficult, even though Indian organizations are making progress. Combining GDPR and DPDP Act suggestions lets firms focus on core compliance and keep flexibility during pilot in areas where GDPR standards are difficult to apply. This dual method may work. Since organizational factors like data protection leadership and international competence affect compliance performance, Indian enterprises need targeted solutions.

6.4 Discussion of Results: Research Question Three: Legal and Compliance Challenges

This study examined Research Question Three (RQ3) to determine how Indian organisations might adapt their data protection policies to GDPR and DPDP Act compliance. Respondents mentioned data localisation, consent management, and cross-border data flow limits as legal challenges. Notably, 47% of respondents listed data localisation as a major challenge, and 51% cited cross-border data transfer difficulties. These findings show that national data protection rules and global data processing needs are challenging to balance. The DPDP Act and GDPR are difficult to comply with for Indian companies moving abroad. Data localisation requires storing personal data in India, which might upset global technology and cloud service companies. Multinational businesses (MNCs) that rely on global data flows find regional data management complicated. Data localisation difficulties affected GDPR and DPDP Act compliance, according to the study's regression analysis. ERP Compliance issues were higher in organisations with tight data localisation requirements (regression coefficient = -0.30, p-value = 0.04).

Due to regulatory duties around data localization, organizations may find it difficult to handle their data properly in conformity with global data protection regulations, according to growing research.

Due to data localization laws, organizations must build and manage separate infrastructure for numerous areas, which increases operational costs and complexity. Organizations had less trouble with GDPR and DPDP Act authorization management requirements, but data localization remained the biggest regulatory challenge. Both data protection systems need informed consent to acquire, handle, or transmit personal data. Organizations must obtain consent before conducting these actions.

Consent management was a major compliance issue for 47% of respondents. The regression study showed a weaker link between compliance and consent (coefficient = -0.22, p-value = 0.08) than data localization issues. Despite their acknowledgement of the importance of authentic consent, companies may struggle to create and implement consent management systems that comply with domestic and international law. Organizations often struggle to gather consent clearly and preserve documents to prove compliance during audits.

The constant tension between international data flows and domestic regulatory demands makes it difficult for businesses to comply with the GDPR and DPDPA, according to this study. Despite Indian organisations' understanding of compliance, the lack of a strong national framework exacerbates these issues. Synergy between international and local data protection standards is needed to improve compliance and operational efficiency. The GDPR encourages data freedom across borders, however national laws like the DPDP Act restrict data management, particularly localisation. This friction forces businesses to choose between local and international data protection rules making the two requirements aren't always compatible.

Global Indian ERP enterprises must reconcile GDPR data export restrictions with India's data storage laws when processing or transmitting personal data abroad. Organisations must adapt to shifting data protection laws. Complex regulatory requirements need Indian and foreign regulators to standardise data protection laws. If both sets of rules conflict, companies may spend more and operate inefficiently. This study concluded that inconsistent cross-border data transfer laws made compliance difficult. Unlike India's tougher data flow legislation, the GDPR permits personal data to be transferred outside the EU to nations that fulfil its high data protection standards.

Companies transferring personal data between jurisdictions may face legal challenges due to these discrepancies. Ambiguity can delay data processing, cause noncompliance, and fines. To overcome these issues, Indian regulatory agencies should collaborate with global regulators to create a uniform data protection framework that respects local data sovereignty and unrestricted cross-border data transfer. A thorough data protection plan helps ease compliance and decrease the burden of multiple,

often contradictory legal requirements. Indian organisations, especially multinationals, must invest in scalable and adaptable data protection solutions to comply with new laws.

Cloud-based solutions that meet GDPR cross-border data transfer rules and domestic data residency restrictions may be used. Modern data management systems can track cross-border data exchanges and make data storage and processing transparent. Training and awareness efforts can also improve compliance culture. Creating a centralised compliance system customised to India's regulatory situation should complement these efforts. However, these efforts should be complemented by the development of a centralized compliance framework tailored to India’s unique regulatory landscape. Such a framework should guide organizations in transitioning from mere awareness to actionable compliance, with clear guidelines, best practices, and tools to ensure adherence to GDPR and DPDP requirements. GDPR and DPDP are complicated legislation, so organisations should train compliance and legal professionals to comprehend them.

With changing laws, GDPR and the DPDP Act will assist Indian ERP companies reduce risks and comply. Data localisation, consent management, and cross-border data transfer restrictions are priorities. Organisations may overcome these hurdles and achieve international and domestic data protection standards by building globally harmonised frameworks, implementing strong data protection procedures, and investing in training and technology.

6.5 Discussion of Results: Research Question Four: Framework Development for GDPR and DPDP Compliance

The fourth research question (RQ4) explored how Indian organizations can develop a structured compliance framework for GDPR and DPDP Act requirements. The findings highlight that GDPR compliance difficulties such data storage, authorisation management, consent management, and cross-border data flow limitations —require a systematic approach that have hampered GDPR compliance. A The proposed Privacy Information Management System (PIMS) framework provides practical steps to assist organizations in navigating these regulatory complexities while ensuring effective data protection. The suggested framework starts with identifying the most pressing compliance issues in needs and expectations and their associated privacy risks. Statistics show Indian companies suffer most with data storage and cross-border data limitations. The framework elements ensure that organisations focus on the most relevant compliance areas. Management of consent and data localisation helps minimise GDPR and DPDPA related compliance challenges.

Smaller organizations are more likely to struggle with compliance; thus, the second component of the framework targets them. The study's regression analysis showed that smaller organizations struggle with compliance due to resource and expertise constraints. The framework recommends creating small-firm-specific compliance requirements to simplify compliance. Data storage instructions, simpler consent management, and examples of required documents may be recommended. Smaller companies sometimes lack the resources to create sophisticated data protection rules; thus, the goal is to simplify compliance for organizations of various sizes.

In the third step, we recommend campaigns to raise awareness on data privacy and capacity building for organizational responsibilities. Smaller companies sometimes lack awareness and resources to understand data protection requirements, unlike larger companies with internal procedures and teams to ensure compliance. Through concentrated efforts, regulators can educate organizations, particularly small enterprises, about data protection regulations, the repercussions of non-compliance, and how to navigate the GDPR and DPDP Act.

To better illustrate the structure of this framework, Figure 17 and 18 (below) presents the proposed Privacy Information Management System (PIMS) process flow, which incorporates essential GDPR and DPDP Act compliance elements. The framework covers key roles such as PII controllers, processors, compliance planning, privacy risk assessment, operational processes, support mechanisms, and continuous improvement strategies. The surveyed organizations responded positively to the proposed framework, with an average acceptance rating of 4.2 out of 5. Many participants acknowledged the framework’s feasibility but highlighted the need for additional technological infrastructure and training programs to facilitate smooth implementation. Some respondents said organisations will need IT infrastructure-dependent compliance tools such automated permission management systems, encryption solutions, and cross-border data transfer protocols. Additionally, respondents underlined the significance of continual staff training for optimal implementation.

The concept suggests a promising way to close study compliance gaps. Organizations’ effectiveness depends on their ability to integrate resources and infrastructure. The report identified data localization and cross-border data flow as issues that require more than new legislation. Instead, organizations should develop comprehensive strategies to address technological challenges (such encrypted data storage and international data transfer protocols) and human capital issues (like compliance training and best practices). organizations need senior leadership commitment to the framework and sufficient resources to implement it. Smaller organizations will need industry group assistance or digital company cooperation to meet compliance standards without straining operations.

Indian regulators and international entities must collaborate for regulatory success. Bringing data protection laws into line with international standards like the GDPR will ease compliance for Indian and multinational firms. Regulatory agencies should aid smaller organizations, who may not have the technical knowledge to fully implement data protection safeguards, and ensure everyone understands compliance obligations. The framework provides a systematic and realistic approach to compliance, but it should be utilized in conjunction with bigger legislative changes that address Indian firms' specific challenges. The structure must be adaptable to local and international needs. The framework may be less beneficial for smaller organizations with less resources without these improvements. The study found that the proposed framework solves Indian organizations' main GDPR and DPDP Act compliance issues.

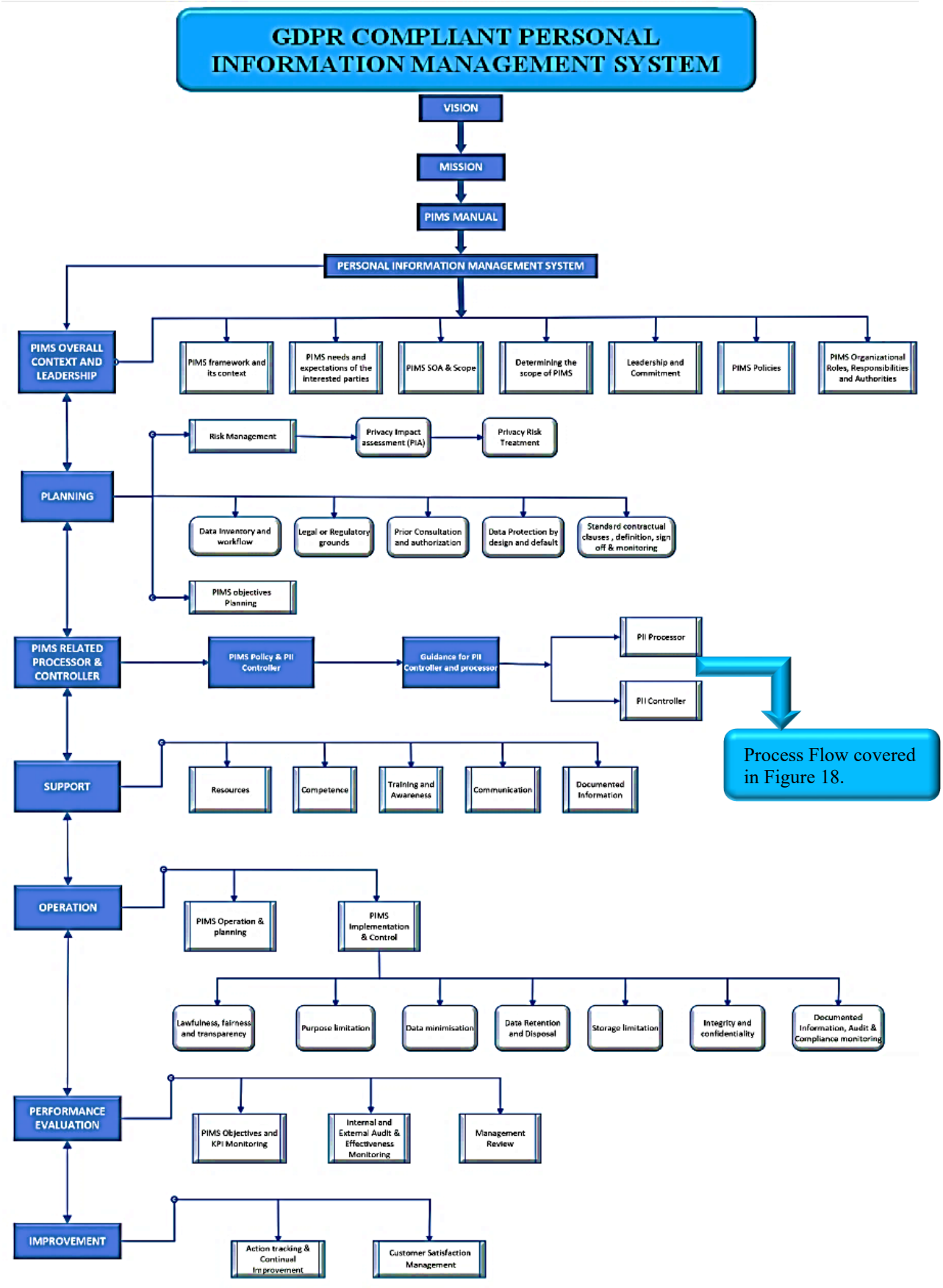
The framework focusses on data storage, consent management, and cross-border data transfer to give companies realistic guidelines. Organizations require the necessary infrastructure, resources, and training to succeed. National and international regulatory bodies must cooperate to simplify data protection laws for businesses and ensure their long-term success and sustenance for privacy compliance.

Table 20:Terminology mapping for GDPR, DPDP Act and Proposed Privacy Information Management System

Terminology	**GDPR**	**DPDP Act**	**Proposed Privacy Information Management system**
Personal Data/ Sensitive Data	*PII*	*PII*	*PII*
Data Subject (Natural Person)	*Data Subject*	*Data Principal*	*PII Principal*
Data controller	*Data controller*	*Data Fiduciary*	*PII Controller*
Data Processor	*Data Processor*	*Data Processor*	*PII Processor*

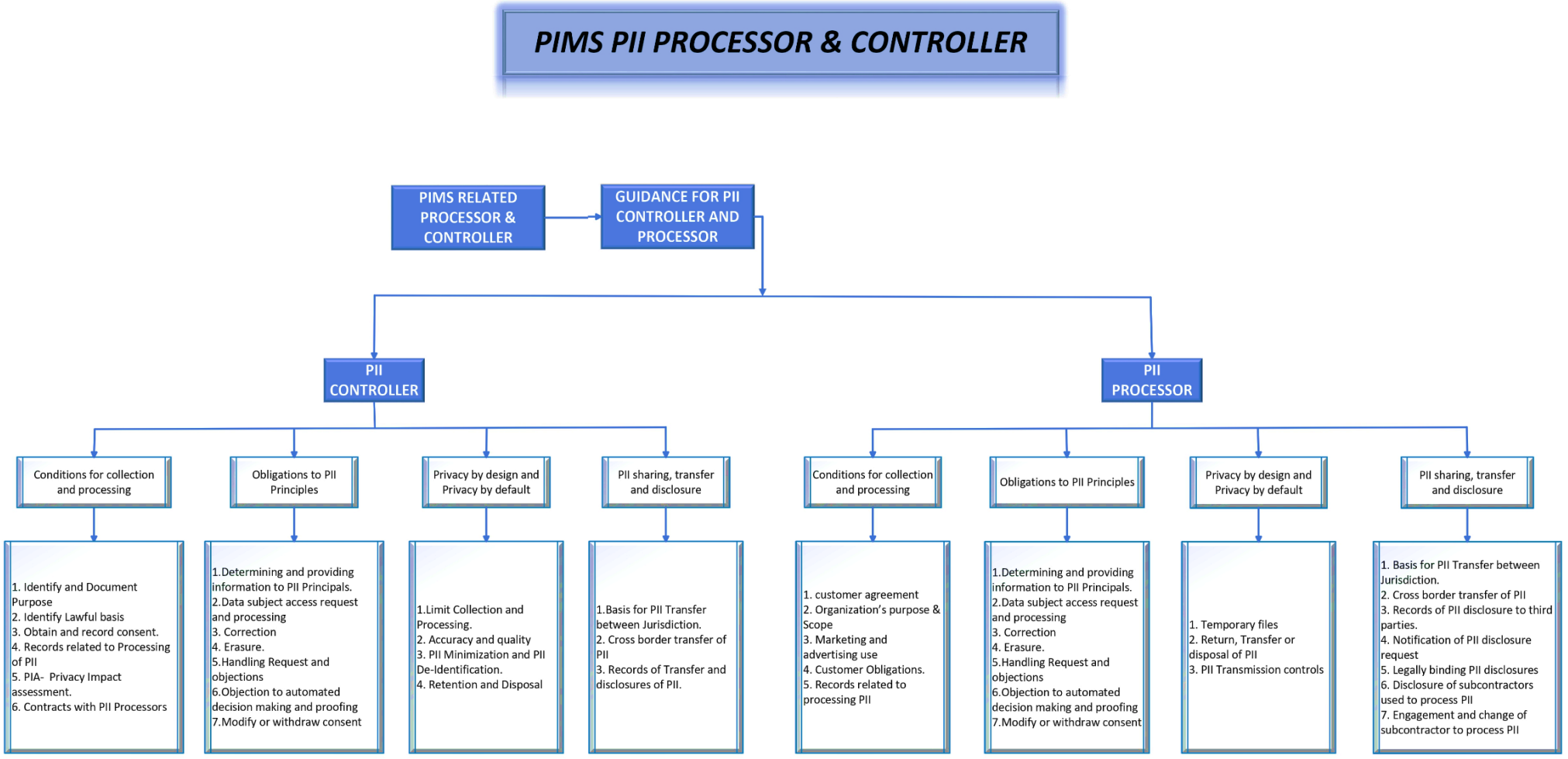
Source: (Shekhar and Choudhary, 2022; DR. Reeta, 2023)

Figure 39: Proposed Framework for GDPR Compliant Personal Information Management System



Source: Author's own work

Figure 40: Proposed Framework for GDPR Compliant Personal information Management system covering PII controller and PII Processor Key Expectations



Source: Author's own work

6.6 Limitations of the Study

In academic research, acknowledging limitations is an essential aspect of providing a transparent and realistic interpretation of the study's findings. This section aims to identify and explain the limitations of the current study, particularly focusing on aspects such as participant-related constraints, data access limitations, and biases that could affect the generalizability of the results. A comprehensive understanding of these limitations will help contextualize the findings and provide directions for future research.

6.6.1 Participant-Related Limitations

As discussed in Section 3.10.1 (Key Limitations), this study primarily relies on self-reported data from industry stakeholders which is one of the main limitations towards participant-related constraints. This introduces a major participant-related limitation as there could be biases in how participants report their GDPR compliance status. Some participants might underreport non-compliance or overstate adherence due to reputational concerns or the desire to present their organizations in a positive light. The sample size for this study was limited to organizations operating within India, which may not fully capture the diversity of experiences from organizations in other countries. While the sample size of 100 participants is sufficient for a cross-sectional study, it may not be large enough to ensure the findings are representative of all types of organizations (small, medium, large) across different sectors (e.g., IT, manufacturing, healthcare). Additionally, the demographics of the participants, including their level of experience with data protection regulations and their role in the organization, could impact the findings. For instance, responses from data controllers may differ from those of data processors, and organizations with a stronger focus on compliance might report different challenges compared to organizations with limited knowledge or resources for data protection. These participant-related limitations mean that the findings may be skewed toward certain types of organizations or specific sectors, reducing the external validity of the study.

6.6.2 Data Access Limitations

Another limitation concerns the difficulty in accessing certain data points, particularly when it comes to organizational training protocols and technical infrastructure recommendations. These aspects of GDPR and DPDP Act compliance are often proprietary to organizations, and accessing detailed information about internal compliance practices can be challenging. This could lead to gaps in the data collected, especially regarding how organizations implement or plan to implement certain compliance measures. Furthermore, some participants may have been reluctant to provide detailed responses about their internal compliance processes due to concerns about confidentiality or regulatory scrutiny, which could have resulted in the underreporting of challenges or an overestimation of their compliance levels.

6.6.3 Bias in Responses

Response bias was another limitation in this study. Respondents from larger organizations or those with dedicated compliance teams may report more favourable or optimistic compliance scores for GDPR compliance status, as they have more resources and established procedures in place. On the other hand, smaller organizations with fewer resources may have been less likely to fully respond to surveys or may have provided responses that downplayed their challenges to avoid being perceived as non-compliant. The study attempted to mitigate this bias by targeting a range of organizations across different sectors and sizes; however, some bias may still be present due to these disparities in resources and focus on compliance.

6.6.4 External Validity and Generalization

The external validity of the study refers to how well the findings can be generalized to a broader context outside the study's sample. Since the sample was limited to Indian organizations, the findings may not fully represent the experiences of organizations in other countries, especially those with different data protection regulations or cultural attitudes toward privacy. For instance, GDPR and the DPDP Act are specific to European and Indian legal frameworks, respectively, and organizations in other regions with different regulatory environments might face different challenges.The challenges identified, such as data localization and cross-border data flow, may not be as pronounced in countries where these issues are less stringent or where local data protection regulations differ from the GDPR and DPDP Act. Therefore, while this study provides valuable insights into GDPR compliance in India, the findings should be interpreted with caution when considering their applicability to other regions or countries.

6.6.5 Impact of DPDP Act Non-Implementation

A key limitation of this study is the fact that while the DPDP Act has been accepted by the Indian government, it has not been implemented, and no timeline has been defined for its enforcement. This lack of clarity leaves Indian organizations in a state of uncertainty about the future of data protection laws. As a result, businesses continue to rely primarily on GDPR for compliance, as it remains the most established framework for data privacy. Until the DPDP Act is enforced and further clarified, GDPR continues to serve as the key standard for privacy assurance in Indian organizations. Without a national framework, this gap creates challenges for Indian ERP companies in aligning their practices with both domestic and international regulatory standards.

To conclude, this chapter discussed the findings from all research questions and connected them with existing studies and regulatory frameworks. It outlined both the progress and continuing challenges in GDPR and DPDP Act compliance among Indian ERP firms, showing how factors such as company size, available resources, and international exposure impact compliance practices. The discussion also reinforced the practical value of the

proposed Privacy Information Management System (PIMS) framework as a way to strengthen compliance and promote more structured data-governance practices.

The next chapter concludes the study by summarizing the key insights, reflecting on the implications of the proposed framework, and presenting recommendations for organizational practitioners, policymakers, and future researchers.

CHAPTER VII: SUMMARY, IMPLICATIONS AND RECOMMENDATIONS

7.1 Summary

In vision of the complex GDPR and the relatively new DPDP Act in India, this study examined Indian software enterprises' GDPR compliance challenges and changes. The DPDP Act has been accepted by the Indian government but, as of now, has not yet been fully implemented, and there is no defined timeline for its full enforcement. As a result, GDPR remains the primary framework for privacy assurance for Indian companies handling data both within India and across borders. The research indicates that while Indian companies are increasingly becoming more aware of the need for data protection under both DPDP Act and GDPR, the lack of a clear, actionable national privacy framework hampers their ability to achieve full privacy compliance. Without a structured and actionable framework for the DPDP Act, the GDPR continues to be the crucial to building a robust privacy assurance framework for Indian businesses, particularly in sectors that interact with the European market. The research aim was to understand how Indian organizations handle compliance challenges, if their procedures match GDPR rules, and how effectively a GDPR-based privacy assurance framework might work for them. The research employed descriptive and inferential statistical techniques to uncover GDPR compliance characteristics and key issues with Indian ERP implementation organizations.

Indian companies demonstrate a growing awareness of data protection rules such as the DPDP Act and GDPR. However, the findings reveal a crucial gap: while there is significant considerate of the standing of data privacy, a robust and cohesive compliance framework is still missing. This absence of a structured approach is holding back India from aligning completely with global standards like GDPR, especially in areas like consent management, data localization, and cross-border data flows. The research underscores the need for a comprehensive national framework that bridges the gaps between awareness and actual implementation. Such a framework should include simplified compliance guidelines, scalable technological solutions, and targeted training programs to equip organizations of all sizes with the tools they need to meet international standards. Without addressing this missing piece, the efforts of Indian organizations to achieve GDPR compliance will remain fragmented and incomplete.

Greater GDPR compliance was seen in larger companies and those with global market expertise. The study's GDPR alignment approach proposed was practicable, but smaller firms worried about adoption owing to resource constraints, cost and awareness. The framework includes legal, technical, and organizational elements. Research Question One revealed that smaller Indian companies cannot meet GDPR criteria owing to financial and resource constraints. The second research question found that companies struggled to execute

GDPR explicit consent standards, particularly in transparency and consent management. The studies also showed that dedicated data security officers and international clientele were found to boost compliance rates.

These findings emphasize the need for innovative and sustainable approaches to address Indian organizations' GDPR compliance challenges, especially in balancing cost, capacity, and international expectations. Indian companies serving global clients are often required to meet stringent GDPR standards, which impose additional financial burdens not typically budgeted for by SMEs. While such compliance enhances trust and international competitiveness, the associated costs of hiring data officers, training staff, and implementing consent systems raise concerns on the ownership. It is worth considering whether part of this investment should be supported by international clients who demand such compliance highlighting a need for more equitable distribution of responsibility in cross-border data partnerships.

Apart from sharing the cost of compliance, there could also be a need for a practical, severity-based approach to GDPR and DPDP implementation. This means that compliance expectations should depend on a company's size, the type and nature of data it handles, and the level of risk involved. Smaller firms that process limited or low-risk data could focus on basic privacy safeguards like consent and breach reporting, while larger organizations or those handling sensitive data should adopt stronger controls and audits. Such a balanced approach would make compliance more realistic, encourage wider adoption, and prevent smaller firms from being overburdened by requirements meant for global enterprises.

As detailed in Table 1 (*Impact on GDP Growth and Data Privacy)* of the Introduction section, the lack of a robust data protection framework, such as the DPDP Act, has had a noticeable negative impact on the growth of India's IT sector and its GDP Contributions. The absence of full GDPR and DPDP compliance poses risks to the sector's growth, potentially limiting India's contributions to its GDP and its standing in the global digital economy. Beyond business challenges, these findings also have broader regulatory and policy implications, underscoring the need for targeted legal reforms and compliance support mechanisms. The findings also have significant theoretical and practical implications for both Indian enterprises and policymakers. The next section explores how this research contributes to the broader data privacy discourse and what actionable insights it offers for improving GDPR compliance in India.

7.2 Implications

7.2.1 Theoretical Implications

The study contributes to global data privacy literature by examining GDPR compliance in a non-EU country with diverse economic and regulatory landscape dynamics. India's rapid digital transformation and growing data protection environment provide a unique context for GDPR adaption in non-EU nations with evolving privacy rules. GDPR, a European legislation, affects businesses in many situations, notably those in

developing economies. The research highlights both the synergies and gaps between the GDPR and India's DPDP Act, on how GDPR is influencing data protection efforts globally, particularly in emerging economies. This influence makes GDPR being considered for adaptation beyond the EU as a global data protection standard.

The research also illuminates the data privacy literature with respect to firm size, resources, and global exposure effect of GDPR compliance. This analysis confirms past research that demonstrated familiarity with overseas clientele and the availability of required resources helped enterprises outside the EU comply with GDPR. This research focusses on these hurdles and predictions to improve our theoretical understanding of compliance dynamics and reveals some of the factors that may affect GDPR adaptation in diverse organizational contexts.

7.2.2 Practical Implications

Despite major challenges, the study's findings give practical recommendations on navigating GDPR compliance for Indian software ERP enterprises. Information storage security and permission management are high-impact compliance areas that companies should address and align with DPDA. The research also suggests that having dedicated data protection professionals who can drive GDPR-related activities and promote a privacy-focused culture within organizations is crucial.

The report advises reorganising smaller organisations to accommodate privacy-focused roles that can better support GDPR compliance. It also suggests that Indian policymakers consider tailoring GDPR-related strategies to align with domestic economic conditions. Offering tiered compliance or easing reporting requirements for SMEs may enable them to meet data protection standards without undue strain.

Additionally, adopting a proportional, severity-based compliance approach where expectations are scaled according to company size, data sensitivity, and operational risk would make GDPR and DPDP implementation more practical for diverse organizations while maintaining regulatory integrity. Smaller organisations could benefit from improved support systems, including affordable training initiatives. Given persistent budgetary limitations, both regulatory bodies and international clients who demand GDPR compliance from Indian service providers should jointly facilitate such efforts through technical assistance, co-funded training, or capacity-building programs that ensure globally compliant data practices without overburdening SMEs and ensuring compliance.

7.3 Recommendations for Future Research

This study examined software companies in India, but future research might include additional Indian enterprises to better understand GDPR compliance challenges across different sectors. Sectors such as finance, healthcare, and e-commerce handle substantial volumes of sensitive personal data and may face unique GDPR challenges. Comparing India's GDPR compliance with that of other emerging economies like Brazil, South Africa, and Indonesia could offer insights into how different regulatory environments affect GDPR adoption. Cross-country comparisons would help developing markets identify best practices and frameworks for GDPR adaptation.

Despite the positive findings, the GDPR-based privacy assurance architecture needs more empirical testing. Future research could pilot the framework's components within Indian organizations to determine its implementation impacts and GDPR compliance outcomes. Data protection officials, lawyers, and IT specialists may provide inputs during framework piloting to ensure the framework is comprehensive and aligns to all key organizational tasks.

To address biases observed in this study, such as larger organizations reporting more favorable compliance scores, future research could incorporate direct compliance audits, independent reviews, or regulatory enforcement data to mitigate response biases and provide a more accurate picture of compliance levels across various organization sizes and sectors. Expanding the sample size to include a broader range of organizations, particularly small and medium-sized enterprises (SMEs), would improve representativeness. Stratifying the sample by company size, industry, and geographic location could help capture a more precise understanding of compliance challenges. Furthermore, future research could explore industry-specific GDPR challenges in India, particularly in sectors like finance, healthcare, and e-commerce, as these sectors handle high volumes of sensitive personal data and may face unique regulatory and operational constraints distinct from those in software ERP Organizations.

Stronger integration between the GDPR and the DPDP Act could significantly streamline compliance processes for Indian businesses in the long run. Future research could examine how DPDP Act changes affect GDPR compliance and how much they replace or enhance GDPR obligations. A deeper investigation into the relationship between the GDPR and the DPDP Act could yield insights into how dual compliance might simplify processes for Indian businesses. By researching this shifting relationship and suggesting dual compliance legislation, researchers could assist Indian organizations adjust. This study would add to the international discourse on GDPR and national legislation and may help influence regulatory responses in non-EU countries with similar challenges.

Collaboration with regulatory bodies such as the DPAI could also provide valuable insights into enforcement mechanisms, compliance trends, and regulatory perspectives on GDPR adaptation in India. Understanding both the organizational and regulatory viewpoints would create a more comprehensive understanding of the compliance landscape. Finally, testing the GDPR-based privacy assurance methodology in real-world Indian organisation case studies could yield relevant actionable data. This would analyse the framework's compliance improvement and reveal how organisations might overcome operational challenges in implementing GDPR-based practices in operations. By addressing these areas, future research can offer a more novel understanding of GDPR compliance challenges, particularly in the context of developing economies like India, and contribute to the ongoing discourse on global data protection standards.

7.4 Conclusion

This study answered the research questions and identified Indian ERP installation organizations' GDPR compliance issues. The research showed that Indian ERP organizations struggle with GDPR owing to cost, resource restrictions, and unfamiliarity. Organizational size, resources, and international market exposure affect GDPR compliance. The study's proposed GDPR-based privacy assurance architecture was positively received, especially its legal compliance section, but it may need some customizations to implement for organizations of different sizes. Indian companies are making GDPR compliance progress, but the results show that smaller companies with lower resources still face significant challenges.

As the DPDP Act in India continues to evolve, aligning it more closely with GDPR could simplify compliance for Indian businesses, especially those dealing with international clients and their data. However, since the DPDP Act has not yet been fully implemented and lacks a defined enforcement timeline, GDPR remains the primary benchmark for data protection in India. GDPR sets data privacy rules for EU and non-EU countries, bolstering the study's significance. Indian companies must reconcile global standards like GDPR with local rules like the DPDP Act to stay compliant in a digital economy. GDPR compliance in India appears promising, but SMEs may need additional time to adjust to this new environment. As they expand into the global digital economy, Indian enterprises must comply with GDPR to meet global data protection standards and please international clientele.

In the long run, GDPR compliance is not just a lawful requirement but a planned authoritative for India's continued growth in the global market. As evidenced in Table 1 (Introduction section), insufficient compliance measures have already negatively impacted the IT sector's growth and GDP contributions. By highlighting Indian organizations' specific difficulties and presenting practical solutions for policy and compliance, this study lays the framework for future research and regulatory policy actions aimed at strengthening data protection policies and ensuring that India remains competitive in global technology markets. By embracing GDPR principles and aligning with international best practices, Indian companies can enhance their competitiveness, build trust with global clients, and contribute to a more robust data protection ecosystem. In doing so, they not only safeguard sensitive data but also strengthen India's place as a leading technology hub in the worldwide digital economy.

APPENDIX A
LIST OF FIGURES

APPENDIX B

LIST OF TABLES

APPENDIX C
SURVEY COVER LETTER

The following cover letter and Online survey was deployed to collect Responses

Hello!

I hope you're doing well!

I'm Premnath Rajagopalan (PREM), and I'm reaching out to ask for your help with an important research survey.

Your insights are crucial for understanding data protection and privacy compliance in the Indian software industry, focusing on the challenges and measures related to the EU-GDPR and India's DPDP Act.

Your expertise and experience in this sector make your input incredibly valuable. I'd be honored if you could take a moment to fill out the survey.

Plese rest assured that your responses will be treated with the utmost confidentiality and used solely for this study.

Survey link: [https://forms.gle/z1kT9WAcaDKkinFfA]

Your time and insights are immensely valuable to this research, and I genuinely appreciate your consideration.

Thank you in advance for your extensive support, and I eagerly await your participation and response.

Warm regards,

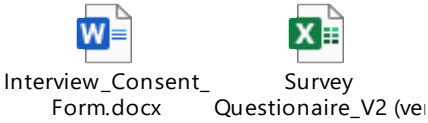
Premnath Rajagopalan (PREM)

Snapshot :

APPENDIX D

INFORMED CONSENT

Similar consent has been intimated and implemented during response collection and during in call discussions.



APPENDIX E

INTERVIEW GUIDE

Survey
Questionaire_V2 (ve

References

1. Abie, H. and Borking, J.J. (2012) *Risk Analysis Methods and Practices Privacy Risk Analysis Methodology Technology Assessment of Dutch DPA Finsec View project*. Available at: https://www.researchgate.net/publication/259471777.
2. Abu-Nimeh, S. and Mead, N.R. (2010) *Combining Privacy and Security Risk Assessment in Security Quality Requirements Engineering*.
3. Agarwal, A. (2020) 'Sanctity of Personal Data : A comparative study of data privacy laws in EU , US and India.', *International Journal of Legal developments and allied issues*, 6.
4. Agrawal, S., Goswami, K. and Chatterjee, B. (2010) 'The evolution of offshore outsourcing in India', *Global Business Review*, 11(2), pp. 239–256. doi:10.1177/097215091001100208.
5. Ahituv, N. and Neumann, S. (2002) *A system development methodology for ERP systems*, *Article in Journal of Computer Information Systems*. Available at: https://www.researchgate.net/publication/279892587.
6. Ahlin, T. and Zupančič, J. (2001) *Implementation of an integrated Software package*.
7. Albrecht, J.P. (2016) *Foreword by How the GDPR Will Change the World*. Available at: www.lexxion.eu.
8. Alhazmi, A., Asanka, N. and Arachchilage, G. (2021) *I'm all Ears! Listening to Software Developers on Putting GDPR Principles into Software Development Practice*.
9. Ali, M. and Miller, L. (2017) 'ERP system implementation in large enterprises – a systematic literature review', *Journal of Enterprise Information Management*. Emerald Group Publishing Ltd., pp. 666–692. doi:10.1108/JEIM-07-2014-0071.
10. Alkubaisy, D. *et al.* (2022) *A Framework for Privacy and Security Requirements Analysis and Conflict Resolution for Supporting GDPR Compliance through Privacy-by-Design*.
11. Alter, S. (1999) 'Enterprise Applications systems', in Alter S (ed.) *Information systems: a management perspective*. Third Edition. Boston, US: Addison-Wesley Longman Inc., pp. 394–406. Available at: https://books.google.co.in/books?id=eOPxAAAAMAAJ&redir_esc=y&hl=en (Accessed: 1 November 2023).
12. Anisimova, A. (2023) 'Indian IT Outsourcing Market. Software Development Outsourcing to India - Blog', *IDAP Group*. Available at: https://idapgroup.com/blog/it-outsourcing-to-india/ (Accessed: 11 October 2023).
13. Anwar, M.J., Gill, A.Q. and Beydoun, G. (2018) 'A review of information privacy laws and standards for secure digital ecosystems', *ACIS 2018 - 29th Australasian Conference on Information Systems* [Preprint]. doi:10.5130/ACIS2018.BB.
14. Arola, P. (2019) *Avoiding GDPR DataBreachA guideline for SAP ERP business systems*.
15. Arora, K. (2020) *Digitalization and Societal Transformation Privacy and data protection in India and Germany: A comparative analysis*. Available at: www.wzb.eu.

16. Aseri, A.M., Abdulah, D.R. and Aseri, M. (2020) 'The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy', *Journal of Theoretical and Applied Information Technology*, 29, p. 4. Available at: https://www.researchgate.net/publication/344243565.
17. Ashraf, S. (2021) *GDPR Implementation Framework for SMEs*.
18. Das Aundhe, M. and Mathew, S.K. (2009) 'Risks in offshore IT outsourcing: A service provider perspective'. doi:10.1016/j.emj.2009.01.004.
19. Bańka, M., Soczyński, T. and Wasiak, D. (2022) 'Practical Methods of Implementation for the Indispensable Mechanism of GDPR Compliance', *Wroclaw Review of Law, Administration & Economics*, 0(0). doi:10.2478/wrlae-2021-0013.
20. Berendt, B.; *et al.* (2017) 'Big data for monitoring educational systems Other How to cite'. doi:10.2766/38557.
21. Bharadwaj, S., Bharadwaj, A.S. and Bendoly, E. (2007) 'The Performance Effects of Complementarities Between Information Systems, Marketing, Manufacturing, and Supply Chain Processes B2B Service Innovation Strategy View project Brainstorming and Ideation in Innovation View project'. doi:10.1287/isre.1070.0148.
22. Bisztray, T. and Gruschka, N. (2019) 'Privacy impact assessment: Comparing methodologies with a focus on practicality', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer, pp. 3–19. doi:10.1007/978-3-030-35055-0_1.
23. Bondre, A., Pathare, S. and Naslund, J.A. (2021) 'Protecting mental health data privacy in india: The case of data linkage with aadhaar', *Global Health Science and Practice*. Johns Hopkins University Press, pp. 467–480. doi:10.9745/GHSP-D-20-00346.
24. Borking, J.J. (2012) *Risk Analysis Methods and Practices Privacy Risk Analysis Methodology*. Available at: https://www.researchgate.net/publication/259471777.
25. Bou Chaaya, K., Allel Hadjali, P. and Djamal Benslimane Mahmoud Barhamgi Pr Bechara Bouna, P. Al (2021) *Privacy Management in Connected Environments*.
26. British Standard Institute (2018) *BS 10012:2017+A1:2018 Data protection. Specification for a personal information management system*.
27. British Standard Institute (2019) *ISO/IEC 27701 Privacy Information ManagementComparing ISO/IEC 27701 and BS 10012August 2019*.
28. Brown, D. and Wilson, S. (2005) 'The black book of outsourcing: how to manage the changes, challenges, and opportunities-John Wiley & Sons, Inc'.
29. Burman, A. (2019) *Will a GDPR-Style Data Protection Law Work for India?*
30. CCPA (2018) *California Consumer Privacy Act (CCPA)*, *, State of California -Department of Justice - , Office of the Attorney General*. Available at: https://oag.ca.gov/privacy/ccpa (Accessed: 18 March 2023).

31. Chand, D. *et al.* (2005) 'A balanced scorecard based framework for assessing the strategic impacts of ERP systems', *Computers in Industry*, 56(6), pp. 558–572. doi:10.1016/j.compind.2005.02.011.
32. Chang, Y. (2010) *The Distinction between 'Privacy' and 'Personal Information' Issues of Personal Information Protection Act in Japan The Relation between Privacy and the Protection of Personal Information*. Available at: http://www5.cao.go.jp/seikatsu/kojin/chousa07/all.pdf.
33. Chatterjee, D. (2021) 'Data Protection Laws In India: Need Of the Hour', *Law Essentials Journal*, 1(1). Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---india.
34. Chaturvedi, A. and Sinha, A. (2017) 'GDPR and India', *The Centre for Internet and Society*, 1(1), pp. 3–20. Available at: https://cis-india.org/internet-governance/blog/gdpr-and-india-a-comparative-analysis (Accessed: 1 November 2023).
35. Clarke, N. *et al.* (2018) 'GDPR: an impediment to research?', *Irish Journal of Medical Science* [Preprint]. doi:10.1007/s11845-019-01980-2/Published.
36. CNIL (2020) *CNIL Stresses Importance of ISO 27701 for Global Data Protection Compliance | Privacy & Information Security Law Blog*. Available at: https://www.huntonprivacyblog.com/2020/04/06/cnil-stresses-importance-of-iso-27701-for-global-data-protection-compliance/ (Accessed: 25 February 2023).
37. Comforte cyberedge group (2020) 'How Data Security Enables Cross-RegulatoryCompliance for Payment Service Providers'.
38. Cynthia J. Rich (2023) 'Get Ready for India's New Data Privacy Law | Morrison Foerster', *Morrison Foerster*. Available at: https://www.mofo.com/resources/insights/230911-get-ready-for-indias-new-data-privacy-law (Accessed: 11 October 2023).
39. Czarnocki, J. *et al.* (2019) *Government access to data in third countries Final Report*. Available at: www.milieu.be.
40. Dashti, S. and Ranise, S. (2020) 'Tool-assisted risk analysis for data protection impact assessment', in *IFIP Advances in Information and Communication Technology*. Springer, pp. 308–324. doi:10.1007/978-3-030-42504-3_20.
41. Davenport, T.H. (1998) *Putting the Enterprise into the Enterprise System*.
42. Davidson, R. (2023) 'ERP Market Share, Size, and Trends Report for 2022', *Software Connect* [Preprint]. Available at: https://softwareconnect.com/erp/erp-market/ (Accessed: 12 February 2023).
43. Decroix, K. *et al.* (2013) *A Framework for Formal Reasoning about Privacy Properties Based on Trust Relationships in Complex Electronic Services*.
44. Degerman, I., Eckerbom, J. and Gu, A.H. (2019) *How do B2B companies approach CRM and the management of customer data in today's era of social media and GDPR? A Multiple Case Study*.

45. Deshmukh, P.D., Thampi, G.T. and Kalamkar, V.R. (2015) 'Investigation of quality benefits of ERP implementation in Indian SMEs', in *Procedia Computer Science*. Elsevier B.V., pp. 220–228. doi:10.1016/j.procs.2015.04.247.
46. Dibbern, J., Winkler, J. and Heinzl, A. (2008) 'Explaining Variations in Client Extra Costs between Software Projects Offshored to', *Source: MIS Quarterly*, 32(2), pp. 333–366.
47. DR. Reeta, V. (2023) *Digital Personal Data Protection Act 2023 - Bill*, *The Gazette of India*. INDIA: Ministry of Law and Justice (Legislative Department). Available at: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf (Accessed: 1 November 2023).
48. Dutta, B. (2021) *An Introduction to the GDPR on European Union Competition Law and its impact on Indian Competition and Privacy Issues*. Available at: https://www.researchgate.net/publication/364331253.
49. Elmuti, D. and Kathawala, Y. (2001) *An overview of strategic alliances*. Available at: http://www.emerald-library.com/ft (Accessed: 28 January 2023).
50. Esteves, J.M. and Pastor, J.A. (1999) 'An ERP Life-cycle-based Research Agenda'.
51. European Commission (2018) *General Data Protection Regulation (GDPR) – Official Legal Text*. Available at: https://gdpr-info.eu/ (Accessed: 7 March 2023).
52. Van Everdingen, Y., Van Hillegersberg, J. and Waarts, E. (2000) *Enterprise resource planning: ERP adoption by European midsize companies | Enhanced Reader*, *Communications of the ACM Volume 43*.
53. Falivene, L. and Falivene, L.I. (2021) *Understanding the Privacy Awareness Gap*. Available at: https://haveibeenpwned.com/.
54. Fatehi, F. *et al.* (2020) 'General data protection regulation (GDPR) in healthcare: Hot topics and research fronts', in *Studies in Health Technology and Informatics*. IOS Press, pp. 1118–1122. doi:10.3233/SHTI200336.
55. Fritsch, L. and Abie, H. (2008a) *Road Map to the Management of Privacy Risks in Information Systems*, *Lecture Notes in Informatics LNI*. Available at: www.nr.no.
56. Fritsch, L. and Abie, H. (2008b) *Towards a Research Road Map for the Management of Privacy Risks in Information Systems*. Available at: www.w3c.org.
57. Gartner (2019) '2019 - Gartner Says Organizations Must Review Outsourcing Arrangements to Mitigate Geopolitical Risk', *Gartner Inc*.
58. Gartner (2021) *Gartner® Recognizes Microsoft as a Leader in the 2021 Gartner Magic Quadrant™ for Cloud ERP for Product-Centric Enterprises - Microsoft Dynamics 365 Blog*. Available at: https://cloudblogs.microsoft.com/dynamics365/bdm/2021/09/13/gartner-recognizes-microsoft-as-a-leader-in-the-2021-gartner-magic-quadrant-for-cloud-erp-for-product-centric-enterprises/ (Accessed: 2 April 2023).

59. Gartner (2022a) ‘Gartner Forecasts India Application Software Spending to Grow 15% in 2022’. Available at: https://www.gartner.com/en/newsroom/press-releases/2022-08-24-india-software-spending-forecast (Accessed: 20 March 2023).
60. Gartner (2022b) *Gartner’s 2022 Predictions for ERP*. Available at: https://www.rootstock.com/cloud-erp-blog/gartners-2022-predictions-for-erp/ (Accessed: 20 March 2023).
61. Gellman, R. (2002) *How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*. Available at: http://www.cdt.org/publications/dmfprivacy.shtml.
62. Ghosh, J. and Shankar, U. (2016) *’Privacy and Data Protection Laws in India: A Right-Based Analysis*. Available at: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspxArticle.
63. Gonzalez-Granadillo, G. *et al.* (2021) ‘Automated cyber and privacy risk management toolkit’, *Sensors*, 21(16). doi:10.3390/s21165493.
64. Greenleaf, G. (2020) *India’s data privacy Bill: Progressive principles, uncertain enforceability*. Available at: https://ssrn.com/abstract=3539432.
65. Gruschka, N. *et al.* (2019) ‘Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR’, in *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*. Institute of Electrical and Electronics Engineers Inc., pp. 5027–5033. doi:10.1109/BigData.2018.8622621.
66. Guaman, D.S., Del Alamo, J.M. and Caiza, J.C. (2021) ‘GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps’, *IEEE Access*, 9, pp. 15961–15982. doi:10.1109/ACCESS.2021.3053130.
67. Gupta, B.K. (2019) ‘General Data Protection Regulation and its Impact on Indian Enterprises’, *AKGEC International Journal of Technology*, 11(1), pp. 28–31. Available at: https://www.akgec.ac.in/wp-content/uploads/2020/10/4-Dr_Brijesh_Kumar.pdf (Accessed: 21 January 2023).
68. Gupta, G. and Joseph, S. (2020) ‘Challenges In Corporate Governance In The Implementation Of GDPR For IT Start-Up Companies In India’, *PalArch’s Journal of Archaeology of Egypt/Egyptology*, 17(9). Available at: https://archives.palarch.nl/index.php/jae/article/view/3999/3938 (Accessed: 2 November 2023).
69. Hadidi, M. *et al.* (2020) ‘Comparison between cloud ERP and traditional ERP’, *Journal of Critical Reviews*, 7(3), pp. 140–142. doi:10.31838/jcr.07.03.26.
70. Halbach, J. (2020) *The German Framework of Personal Data Protection*. doi:10.13140/RG.2.2.23792.17924.
71. Harding, A. (2018) *EasyChair Preprint An Agile Approach to GDPR Implementation within a Further Education College*.
72. Heckle, R.R. and Holden, S.H. (2006) ‘Analytical Tools for Privacy Risks: Assessing Efficacy on Vote Verification Technologies’. Available at: http://www.sims.berkeley.edu/ (Accessed: 26 January 2023).

73. Herrle, J. and Hirsh, J. (2019) ‘The Peril and Potential of the GDPR -’, *Centre for International Governance Innovation*. Available at: https://www.cigionline.org/articles/peril-and-potential-gdpr/?utm_source=google_ads&utm_medium=grant&gclid=CjwKCAiAiKuOBhBQEiwAId_sKx4DwmFRkN1d0lTnx2j1sbjytYgf5vVu5QJeRnvgXOT8WIRxGPf63xoCPlMQAvD_BwE (Accessed: 19 March 2023).
74. Hirvonen, P. (2022) *A Review of GDPR Impacts on Information Security*. Available at: http://rightsstatements.org/page/InC/1.0/?language=en.
75. Hrischev, R. (2020a) ‘ERP systems and data security’, in *IOP Conference Series: Materials Science and Engineering*. Institute of Physics Publishing. doi:10.1088/1757-899X/878/1/012009.
76. Hrischev, R. (2020b) ‘ERP systems and data security’, in *IOP Conference Series: Materials Science and Engineering*. Institute of Physics Publishing. doi:10.1088/1757-899X/878/1/012009.
77. Hussain, F. *et al.* (2019) ‘Enterprise API Security and GDPR Compliance: Design and Implementation Perspective’. Available at: http://arxiv.org/abs/1909.08048.
78. IANS (2022) ‘India’s BPM industry logs $44 bn revenues, grows at 14% in FY22: Report’, *The Statesman*. Available at: https://www.thestatesman.com/business/indias-bpm-industry-logs-44-bn-revenues-grows-at-14-in-fy22-report-1503120442.html (Accessed: 21 June 2023).
79. Impelsys (2019) *GDPR (Regulation) & PIMS (BS 100012 Standard) Overview*. Bangalore. Available at: https://www.impelsys.com/wp-content/uploads/2022/04/GDPR-and-PIMS-Overview.pdf (Accessed: 3 November 2023).
80. International Organization for Standardization (2013) *ISO 27001:2013 -Information technology — Security techniques — Information security management systems — Requirements*.
81. Javeria Anwar, M. and Qumer Gill, A. (2020) ‘Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model’, in *Australasian Conference on Information Systems* . Wellington: Australasian Conference on Information Systems, pp. 1–12. Available at: https://opus.lib.uts.edu.au/rest/bitstreams/fcd809e8-4f81-496f-b111-101330b33845/retrieve (Accessed: 3 November 2023).
82. Al Jazeera (2022) *India withdraws data protection and privacy bill*, *Business and Economy News* . Available at: https://www.aljazeera.com/economy/2022/8/4/india-withdraws-data-protection-and-privacy-bill (Accessed: 9 March 2023).
83. Jha, V.K. and Pal, P. (2016) *Literature review on ERP implementation challenges*, *Int. J. Business Information Systems*.
84. Johnson, E. (2011) *Privacy Maturity Model*. Available at: www.copyright.com.
85. Karyda, M. (2018) *An evaluation framework for privacy impact assessment methods*. Available at: https://www.researchgate.net/publication/326723199.

86. Kawintiranon, K. and Liy, Y. (2021) ‘Towards Automatic Comparison of Data Privacy Documents: A Preliminary Experiment on GDPR-like Laws’, in *SIGITE 2017 - Proceedings of the 18th Annual Conference on Information Technology Education*. Association for Computing Machinery, Inc, pp. 39–40. doi:10.1145.

87. Kedia, B.L. and Lahiri, S. (2007) ‘International outsourcing of services: A partnership model’, *Journal of International Management*, 13(1), pp. 22–37.

88. Khaleel, Y. and Sulaiman, R. (2013) ‘A system development methodology for ERP system in SMEs of Malaysian manufacturing sectors Analysis of GPS data for Public Transporation’, *Article in Journal of Theoretical and Applied Information Technology*, 20(2). Available at: https://www.researchgate.net/publication/287949988.

89. Kolekar, Y.P. (2015) *Protection of data under Information Technology law in India*. Available at: http://www.telegraphindia.com/1140429/jsp/frontpage/story_18290520.jsp#.VKPPqdKUduA.

90. Korff, D. and Douwe Korff (2016) *Practical Implications of the new EU General Data Protection Regulation for EU-and non-EU Companies*. Available at: https://ssrn.com/abstract=3165515www.korff.co.uk/douwedouwe@korff.co.uk1.

91. Kozhukhivskyi, A.D. and Kozhukhivska, O.A. (2022) ‘Risk Assessment Modeling of ERP-Systems’, *Radio Electronics, Computer Science, Control*, (4), p. 149. doi:10.15588/1607-3274-2022-4-12.

92. Kumar, A. (2021) *The Right to be Forgotten in Digital Age: A Comparative Study of the Indian Personal Data Protection Bill*. Available at: https://www.hpnlu.ac.in/journal-level-.

93. Kumar, K. and J Van Hillegersberg (2000) ‘ERP experiences and evolution’, *Communications of the ACM* [Preprint]. Available at: https://go.gale.com/ps/i.do?id=GALE%7CA61792746&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00010782&p=AONE&sw=w (Accessed: 27 January 2023).

94. Kuner, C. (2020) ‘Symposium on the GDPR and international law. The GDPR and international organizations’, in *AJIL Unbound*. Cambridge University Press, pp. 15–19. doi:10.1017/aju.2019.78.

95. Kurt Wimmer, B., Maldoff, G. and Lee Covington, D. (2020) *International Association of Privacy Professionals • iapp.org Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR*. Available at: https://iapp.org/resources/article/comparison-indian-personal-data-protection-bill-2019-vs-gdpr/ (Accessed: 21 January 2023).

96. Lachaud, E. (2020a) ‘ISO/IEC 27701: Threats and Opportunities for GDPR Certification’, *SSRN Electronic Journal*, 1, pp. 1–23. doi:10.2139/ssrn.3521250.

97. Lachaud, E. (2020b) *ISO/IEC 27701: Threats and Opportunities for GDPR Certification*. Available at: https://www.huawei.com/en/press-events/news/2019/12/huawei-ma5800-code-evaluation-build-.

98. Lachaud, E. (2020c) ‘What GDPR tells about certification’, *Computer Law and Security Review*, 38. doi:10.1016/j.clsr.2020.105457.

99. Lachaud, E. (2020d) *What the GDPR Tells about Certification*. Available at: https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-son-projet-de-.
100. Lambe, C.J., Spekman, R.E. and Hunt, S.D. (2002) 'Alliance competence, resources, and alliance success: Conceptualization, measurement, and initial test', *Journal of the Academy of Marketing Science*, pp. 141–158. doi:10.1177/03079459994399.
101. Larsson, A. and Lilja, P. (2019) 'GDPR: What are the risks and who benefits?', in *The Digital Transformation of Labor (Open Access): Automation, the Gig Economy and Welfare*. Taylor and Francis, pp. 187–199. doi:10.4324/9780429317866-11.
102. Laughlin, S.K. (1968) 'Westin: Privacy and Freedom Westin: Privacy and Freedom Recommended Citation Recommended Citation', *Michigan Law Review*, 66.
103. Law, C.C.H., Chen, C.C. and Wu, B.J.P. (2010) 'Managing the full ERP life-cycle: Considerations of maintenance and support requirements and IT governance practice as integral elements of the formula for successful ERP adoption', *Computers in Industry*, 61(3), pp. 297–308. doi:10.1016/j.compind.2009.10.004.
104. Lekhi, R. (2021a) 'GDPR compliance- here's what Indian businesses should know', *Pleaders Blog - Lawsikho*, 10 June. Available at: https://blog.ipleaders.in/gdpr-compliance-heres-indian-businesses-know/ (Accessed: 3 November 2023).
105. Lekhi, R. (2021b) *GDPR compliance: here's what Indian businesses should know*.
106. Li, H., Yu, L. and He, W. (2019) 'The Impact of GDPR on Technology Development', *Journal of Global Information Technology Management* [Preprint].
107. Linden, T. *et al.* (2020) 'The Privacy Policy Landscape After the GDPR', *Proceedings on Privacy Enhancing Technologies*, 2020(1), pp. 47–64. doi:10.2478/popets-2020-0004.
108. Mast, J. (2018) *SAP Authorization Concept renewal project and GDPR in Company X*.
109. Matulevičius, R. *et al.* (2020) 'A Method for Managing GDPR Compliance in Business Processes', in *Lecture Notes in Business Information Processing*. Springer Science and Business Media Deutschland GmbH, pp. 100–112. doi:10.1007/978-3-030-58135-0_9.
110. Mehta, A. (2016) *Understanding Cloud Based ERP Implementation in light of Conventional ERP Implementation at Indian SMEs: a Case Study*. Available at: http://ssrn.com/abstract=2782244Electroniccopyavailableat:https://ssrn.com/abstract=2782244Electroniccopyavailableat:http://ssrn.com/abstract=2782244.
111. Ministry of Statistics and Programme Implementation (2021) *India GDP sector-wise 2021*, *Times of India*. India. Available at: https://statisticstimes.com/economy/country/india-gdp-sectorwise.php (Accessed: 10 October 2023).
112. Mironeanu, C. and Aflori, C. (2021) 'GDPR Records of Processing Activities for Data Controllers', *Bulletin of the Polytechnic Institute of Iaşi. Electrical Engineering, Power Engineering, Electronics Section*, 67(4), pp. 9–24. doi:10.2478/bipie-2021-0019.

113. Nandi, M.L. and Kumar, A. (2016) ‘Centralization and the success of ERP implementation’, *Journal of Enterprise Information Management*, 29(5), pp. 728–750. doi:10.1108/JEIM-07-2015-0058.
114. Nandi, M.L., Kumar, A. and Pai, T.A. (2015) *Centralization and the success of ERP implementation*.
115. Oetzel, M.C. and Spiekermann, S. (2012) ‘Privacy-by-Design through Systematic privacy impact assessment - a design science approach’, *Barzelona* [Preprint]. Available at: http://ssrn.com/abstract=2050872.
116. Oomen, I. and Leenes, R. (2008) *Privacy Risk Perceptions and Privacy Protection Strategies*. Available at: http://www.prime-project.eu.
117. Ramachandran, K. and Voleti, S. (2004) ‘Business Process Outsourcing (BPO): Emerging Scenario and Strategic Options for IT-enabled Services’, *Vikalpa*, 29(1), pp. 49–62. doi:10.1177/0256090920040105.
118. Rana, N. (2022) *Preserving Personal Data - A comparison of Data Privacy Laws in India and the Western World*. Available at: https://knowlaw.in/index.php/2022/07/27/personal-data-comparison-of-data-privacy-laws-in-india-and-the-western-world/ (Accessed: 20 March 2023).
119. Rao, P. (2020) *Personal Data Protection Law in India – Legal Developments*, *Intellectual Property Attorneys, India*. Available at: https://www.legal500.com/developments/thought-leadership/personal-data-protection-law-in-india/ (Accessed: 20 March 2023).
120. Raschke, P. *et al.* (2018) ‘Designing a GDPR-compliant and UsablePrivacy Dashboard’, *HAL Open Science*, p. 978. doi:10.1007/978-3-319-92925-5_14ï.
121. Rieti Ito, E. *et al.* (2019) *Effects of Regulations on Cross-border Data Flows: Evidence from a Survey of Japanese Firms*, *RIETI Discussion Paper Series*. Available at: https://www.rieti.go.jp/en/.
122. Rupčić, N. (2021) ‘Implementing enterprise resource planning in SMEs: the consultants’ perspective’, *International Journal of Business Information Systems*, 37(4), p. 467. doi:10.1504/ijbis.2021.117001.
123. Sable, V. (2020) *Constitutional Validity of Data Protection Bill 2019*. Available at: https://www.researchgate.net/publication/340916702.
124. Saini, S. *et al.* (2010) ‘Success factors for implementing ERP in SMEs in India: A conceptual model’, *IEEE International Conference on Information Management and Engineering 2010* [Preprint]. Available at: https://ieeexplore.ieee.org/abstract/document/5477515/ (Accessed: 27 January 2023).
125. Saxena, S. (2021) ‘Comparative analysis of India’s data protection norms with European Union’s (GDPR) Norms’, *SUPREMO AMICUS*, 23. Available at: www.supremoamicus.org.
126. Schniederjans, D. and Yadav, S. (2006) ‘Successful ERP implementation: an integrative model’, *Rollands and Prakash*, Brown. doi:10.1108/14637151311308358.
127. Sen, P. (2021) *EU GDPR and Indian Data Protection Bill: A comparative study*. Available at: https://gdpr-info.eu/art-1-gdpr/.

128. Shaul, L. and Tauber, D. (2013) *Critical Success Factors in Enterprise Resource Planning Systems: Review of the Last Decade*, *ACM Computing Surveys (CSUR)*. Available at: http://doi.acm.org/????????

129. Shekhar, R. and Choudhary, A. yuvraj (2022) 'Digital Personal Data Protection Bill vis-à-vis GDPR-IndiaCorpLaw'. Available at: https://indiacorplaw.in/2022/11/digital-personal-data-protection-bill-vis-...

130. Sing, E., Matulevičius, R. and Tom, J. (2018) *A Meta-Model Driven Method for Establishing Business Process Compliance to GDPR*.

131. Singh, H.P. (2018) *Data Protection and Privacy Legal-Policy Framework in India: A Comparative Study vis-à-vis China and Australia Digital Technologies View project IT Security View project Data Protection and Privacy Legal-Policy Framework in India: A Comparative Study vis-à-vis China and Australia*. Available at: www.amity.edu.in/ajcs.

132. Singh, M. (2022) 'India withdraws personal data bill that alarmed tech giants', *Tech Giants*. Available at: https://techcrunch.com/2022/08/03/india-government-to-withdraw-personal-data-protection-bill/?guccounter=2 (Accessed: 20 March 2023).

133. Singh Rahul, S. (2023) 'Explained: India's new Digital Personal Data Protection framework', *Hindustan Times*, 3 November. Available at: https://www.hindustantimes.com/technology/explained-indias-new-digital-personal-data-protection-framework-101691912775654.html (Accessed: 25 September 2023).

134. Soliman, M. and Karia, N. (2015) *Higher Education Competitive Advantage: Enterprise Resource Planning Systems*.

135. Sukumar, A. (2017) *Working with 'Last Mile' Data Protection in India*.

136. The BPO Network (2022) 'Pros and Cons of Outsourcing to India', *The BPO Network*, 7 January. Available at: https://www.thebponetwork.com/blog/pros-and-cons-of-outsourcing-to-india (Accessed: 10 October 2023).

137. Upadhyay, P. *et al.* (2010) *A Comparative Study of Issues Affecting ERP Implementation in Large Scale and Small Medium Scale Enterprises in India: A Pareto Approach*, *International Journal of Computer Applications*.

138. Vanezi, E. *et al.* (2019) *GDPR Compliance in the Design of the INFORMe-Learning Platform: a Case Study*.

139. Vayyavur, R. (2015) *International Journal of Current Engineering and Technology ERP Implementation Challenges & Critical Organizational Success Factors*, *2759| International Journal of Current Engineering and Technology*. Available at: http://inpressco.com/category/ijcet.

140. Verizon (2020) *2020 Data Breach Investigations Report in Financial and Insurance industries*. Available at: e: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf ((Accessed: 16 March 2023).

141. Vranaki, A. (2016) ‘Implementing and Interpreting the GDPR: Challenges and Opportunities “Towards a Successful and Consistent Implementation of the GDPR” Centre for Information Policy Leadership Workshop Report’. doi:10.13140/RG.2.2.31789.08163.

142. Wadhwa, R. and Bains, G. (2022) ‘The evolution of India’s data privacy regime in 2021 https://iapp.org/news/a/the-evolution-of-indias-data-privacy-regime-in-2021’, *International Association of Privacy Professionals*. Available at: https://iapp.org/news/a/the-evolution-of-indias-data-privacy-regime-in-2021/.

143. Wankhede, A. (2017) ‘Data Protection in India and the EU’:, *European Data Protection Law Review*, 2(1), pp. 70–79. doi:10.21552/edpl/2016/1/8.

144. Warren, S.D. and Brandeis, L.D. (1890) ‘The Right to Privacy’, *Harvard Law Review*, 4(5), p. 193. doi:10.2307/1321160.

145. Yadav, Dr.A. and Yadav, G. (2021) ‘Data Protection in India in reference to Personal Data Protection Bill 2019 and IT Act 2000’, *IARJSET*, 8(8). doi:10.17148/iarjset.2021.8845.

146. Yasir, S. and Singh, K.D. (2022) ‘India Scraps Data Privacy Bill-The New York Times’, *The New york Times*. Available at: https://www.nytimes.com/2022/08/04/business/india-data-privacy.html.