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

Research Proposal Paper

Author: Premnath Rajagopalan, Swiss School of business Management Geneva, premnath@ssbm.ch

Co-author: PhD Dario Silic, professor, Swiss School of business Management Geneva, University of applied science VSS, dario@ssbm.ch

"Abstract"

In the context of global data protection standards, such as the EU-GDPR, India's software package implementation industry encounters distinct challenges. This research delves into the hurdles faced by Indian software organizations when attempting to meet GDPR requirements and explores the alignment between their data processing practices and the mandates of the EU-GDPR and DPDP Act. Given the complexities of bridging European standards and Indian practices, the study aims to craft a privacy assurance framework tailored to India's unique context. This proposed framework will specifically cater to data processors in the software package industry, addressing their dual need to satisfy EU clients while navigating Indian regulatory specifics. Through this research, a deeper understanding of GDPR compliance within the Indian package implementation sector will emerge, offering solutions to foster heightened data protection measures in line with global standards.

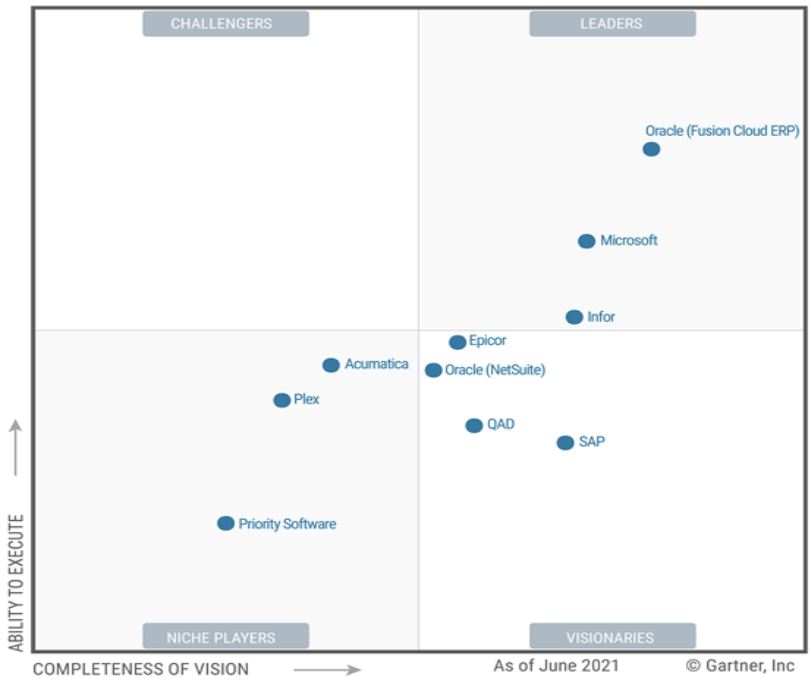
***Keywords**: EU-GDPR, Data Protection, Privacy Assurance Framework, Data Processors, Software Package Implementation in India, DPDP Act, Data Security, Compliance, Client Data Protection.*

1 Introduction

A company's strategy, structure, and 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 modules that can be selected and implemented independently, depending on the specific needs of an organization. These ERP implementations provide custom-made and out-of-the-box packages that can accommodate different business critical modules, such as sales and distribution, materials management, production planning, capital management, customer relationship management, finance management, and 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 Cloud ERP for Product-Centric Enterprises



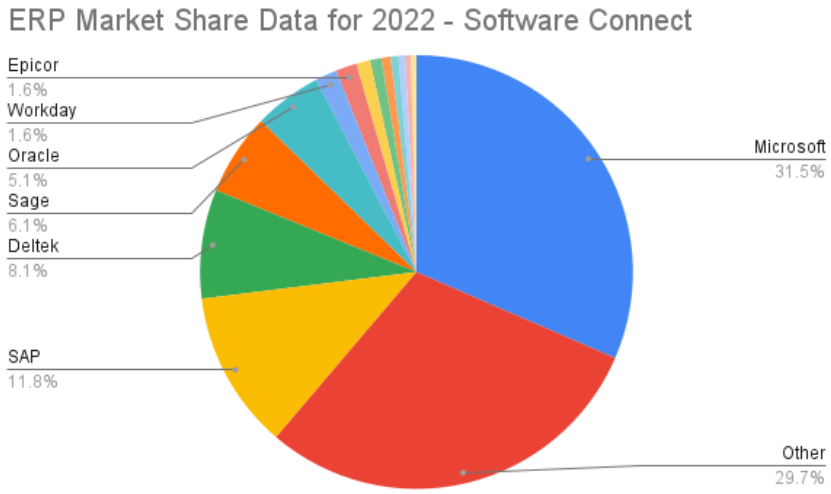
Source: Gartner (August 2021)

In most of the instances of package implementations, the development and deployment for customer 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 Systemanalyse Programmentwicklung (SAP) suite package in North America region collaborating with offshore delivery centre in India for Customer implementation.

Based on recent market reports, Davidson (2022) states that the software package implementation industry in India has witnessed significant growth in recent years and has emerged as a vital contributor to the nation's economy.

Figure 2 – ERP Market Share Data



Source: (Davidson, 2023)

The significant expansion of enterprise package has also posed new challenges, particularly concerning privacy and data protection (Davidson, 2023). The introduction of the European Union's General Data Protection Regulation (GDPR) has led to a higher demand for robust data protection measures, which presents new challenges and potential opportunities for organizations worldwide to improve their data security. The General Data Protection Regulation (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. 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.

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). India's commanding presence, holding 55% of the worldwide IT outsourcing arena, emphasizes the pressing need for a solid data protection framework, with the EU General Data Protection Regulation (EU-GDPR) serving as a potential benchmark(The BPO Network, 2022).

This research paper investigates and develop an EU-GDPR based privacy assurance framework tailored to the unique needs and challenges of data processors in the software package implementation industry in India. By aligning data processing practices with EU-GDPR requirements, Indian companies can enhance data protection, foster international trust, and ensure compliance with global data privacy norms.

2 Problem Statement

Indian software package implementation organizations processing data for EU clients as data processors face significant challenges in complying with (Gupta and Joseph, 2020). 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, 2021). This research aims to identify these challenges and propose solutions for privacy framework preferably for Data processors in software package implementation in India .

3 Research Questions

The following research questions will be focussed for this study:

RQ1: What are the 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 DPDP Act compliance?

RQ4: How can a privacy assurance framework be developed to bridge compliance gaps and facilitate GDPR and DPDP Act compliance for Indian data processors ?

4 Objectives, Variables and Aims

4.1 Overall objective

The overall objective of this research is to enhance data protection compliance in the Indian software implementation industry by analysing GDPR challenges and proposing a new framework tailored to Indian needs preferably in Package implementation industry.

4.2 Specific aims

1. There are basically three specific aims listed below:
2. To identify and analyze the challenges faced by Indian software organizations in complying with GDPR standards as a processor.
3. To explore the relationships between GDPR standards in Europe and Indian organizational practices.
4. To propose a new framework for GDPR compliance with local specificities in India for data processors supporting EU Clients.

4.3 Variables and hypothesis proposed

Dependent variable:

The dependent variable in our research is the level of data protection and privacy compliance among Indian data processors in the software package implementation industry to serve EU clients.

Independent variables:

- EU-GDPR compliance

This variable measures the extent to which Indian data processors comply with the EU General Data Protection Regulation (EU-GDPR) requirements.

- DPDP act compliance

This variable measures the extent to which Indian data processors comply with the Digital Personal Data Protection (DPDP) Act requirements.

4.4 Research question and hypothesis mapping

Research Question	Hypothesis
RQ1: What are the 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?	H1: Indian software organizations face significant challenges in complying with GDPR expectations, and it is possible to adapt GDPR standards 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?	H2: Indian software package organizations exhibit varying degrees of alignment with EU-GDPR and DPDP Act requirements in their data processing practices.
RQ3: What legal and compliance challenges do Indian software package organizations face in achieving EU-GDPR and DPDP Act compliance?	H3: Indian software package organizations encounter legal and compliance challenges that hinder their achievement of EU-GDPR and DPDP Act compliance.
RQ4: How can a privacy assurance framework be developed to bridge compliance gaps and facilitate GDPR and DPDP Act compliance for Indian data processors?	H4: It is possible to develop a privacy assurance framework that can bridge compliance gaps and facilitate GDPR and DPDP Act compliance for Indian data processors.

5 Potential Findings and Issues

5.1 Potential findings

Our preliminary analysis suggests potential findings relevant to the development of an EU-GDPR based Privacy Assurance Framework for Data Processors in the Software Package Implementation Industry in India:

- Indian Data Processors specializing in package implementation, when aligned with GDPR principles, may experience improved access and greater trustworthiness in European markets.

- The software package implementation sector, a vital contributor to India's GDP, underscores the industry's urgent requirement for a robust data protection framework, particularly concerning GDPR compliance.

- Implementing enhanced data protection measures has the potential to attract preferred business partnerships within India, fostering trust and reliability among stakeholders.

5.2 Issues

The software package implementation sector in India faces several critical challenges related to data protection and privacy in the context of GDPR compliance:

- Intellectual Property Concerns: The risk of unauthorized duplication or replication of software codes poses a significant obstacle to data processors.

- Infrastructure Limitations: Some regions in India experience issues with inconsistent connectivity and unreliable network security, impacting the industry's ability to meet data protection standards.

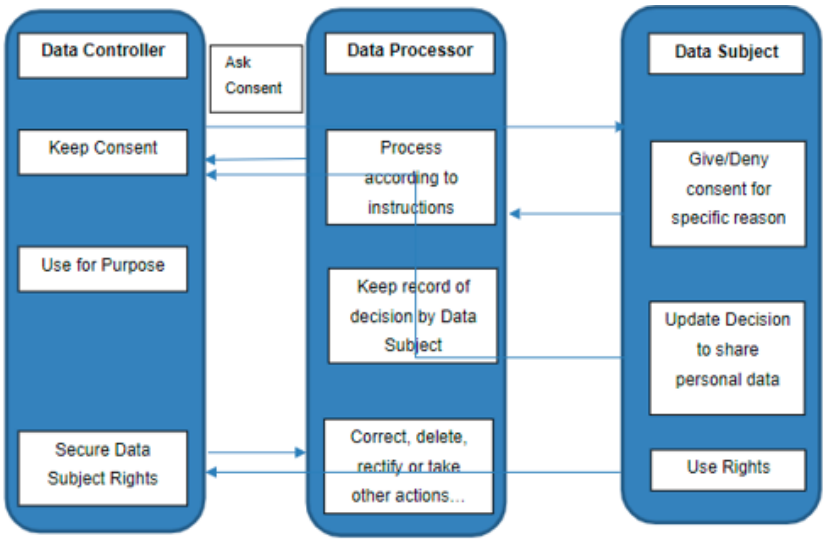
- Cross-Cultural Communication Challenges: The need to align Indian implementation practices with GDPR requirements for European clients can result in communication difficulties, chances on data leakage by processors and misunderstandings during project execution.

- Talent Management Complexities: The abundance of IT professionals can lead to challenges in selecting the right individuals for specific projects, which is crucial for ensuring data security and privacy compliance.

6 Literature Review

The literature review delves into critical aspects of India's software package implementation industry and its evolving data protection landscape, all within the context of the General Data Protection Regulation (GDPR). It encompasses three pivotal domains: Enterprise Resource Planning (ERP) systems, outsourcing alliances, and the changing landscape of data privacy norms. These areas serve as foundational elements in understanding India's technological landscape, its data privacy challenges, and the framework needed for an EU-GDPR-based privacy assurance for data processors in the software package implementation industry.

Figure 1: Data Controller Vs Data Processor Vs Data Subject



Source: (Ashraf, 2021)

The above Data flow (Figure 1) discusses the interaction between a Data Controller and Data Processor concerning data subject's data. The figure also highlights the various key controls that need to be implemented in line with GDPR principles for collecting, handling, and processing data among key stakeholders.

6.1 ERP Systems in India: advancing efficiency and security

The review commences with an exploration of ERP systems, pivotal for optimizing organizational functions. Implementing ERP systems in India entails intricacies, including cost considerations and sustained maintenance (Hrischev, 2020). Notably, India is witnessing a shift toward cloud-based ERP systems, signifying the need for a robust data security framework within ERP deployments(Gupta and Joseph, 2020) .

6.2 Outsourcing alliances: India's IT industry expansion

The literature underscores the strategic significance of outsourcing alliances, extending to cross-border collaborations aimed at cost reduction, operational enhancement, and competence development. India's booming outsourcing sector reflects globalization and technological progress. However, this upward trajectory is accompanied by risks, including communication challenges, evolving regulations, and data security concerns. Gartner's projection that multi-country sourcing approaches will dominate large enterprises' service delivery strategies underscores the industry's dynamism (Gartner, 2022)

6.3 Data Privacy Norms and GDPR: a global benchmark

Data privacy and protection have assumed paramount importance in the digital era, with GDPR setting the international standard. The review highlights the need for robust privacy methodologies and tools to underpin privacy-respecting infrastructures. India's data protection laws, including the IT Act 2000, IT Act 2011, and the prospective Personal Data Protection Bill, are evolving to align with global benchmarks (Yadav and Yadav, 2021).

6.4 Challenges in GDPR Compliance: a focus on ISO standards

The GDPR compliance remains a challenging landscape, and the literature explores various compliance frameworks such as ISO 27001:2013, ISO/IEC 29100:2011, ISO/IEC 27018:2019, and ISO/IEC 27701:2019, all designed to ensure adherence (Lachaud, 2020) ISO/IEC 27701:2019 is poised to emerge as the GDPR certification standard, potentially bolstering organizations' compliance endeavours and market positioning. However, comprehensive guidance regarding its role in achieving holistic GDPR compliance remains a salient concern (Javeria Anwar and Qumer Gill, 2020).

6.5 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 milieu lacks robust legislation, rendering the curbing of user data misuse by product or service companies an intricate challenge (Falivene and Falivene, 2021).

6.6 India's new Digital Personal Data Protection Framework

The recent introduction of India's Digital Personal Data Protection (DPDP) Act marks a transformative phase in data protection. While it empowers individuals (DR. Reeta, 2023) with greater control over their data, the law has sparked debates due to exemptions granted to state entities and potential impacts on press freedom. The DPDP Act lays down stringent obligations for data fiduciaries, outlines the rights and responsibilities of individuals, and introduces special provisions regarding data transfer and government powers. It encompasses personal data in digital form, collected in India or processed abroad when serving Indian individuals (Singh Rahul, 2023) .

6.7 Overall summary

The literature review provides foundational insights into India's technological landscape, data privacy challenges, and the evolving data protection framework for package implementation industries. These findings serve as a precursor to future research that will delve into critical aspects, including the compliance landscape of Indian software organizations with GDPR and the formulation of an EU-GDPR-based privacy assurance framework tailored to India's unique context.

This comprehensive review considers the evolving data protection framework introduced by India's DPDP Act, further cementing the need for an EU-GDPR based privacy assurance framework within the software package implementation industry in India.

7 Research Methodology

7.1 Overview

This research will employ a mixed-methods approach, combining qualitative and quantitative research methods. Data collection will involve surveys and data analysis. The study will target employees, managers, and legal/compliance experts in Indian software package implementation companies.

7.2 Research Methods

7.2.1 Population and study sample

The primary population of interest includes data processors in the software package implementation industry in India. This may include employees, managers, and key stakeholders in various departments within software package organizations who process data relevant to scope of natural person.

To ensure a representative sample, we plan to use the stratified random sampling technique. Stratification can be based on the size of the software package organizations, geographical locations within scope of this research, and types of services offered.

7.2.2 Data collection methods and instruments

Quantitative Data: The plan is to collect quantitative data through structured online surveys. The survey questionnaire will ensure coverage of information related to GDPR compliance, privacy practices, and the challenges faced by data processors in India.

The survey will encompass an assessment of the industry's comprehension of the EU-GDPR, as well as an evaluation of their awareness of challenges such as intellectual property piracy and infrastructure limitations. Furthermore, data collection will encompass 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.

The survey questionnaire shall include closed-ended questions with options for respondents to rate their level of agreement, as well as multiple-choice questions aligning to our research goals and hypothesis. This will help to quantitatively analyze the extent of GDPR compliance and identify any gaps.

To gain deeper insights, we may also consider random semi-structured interviews with key informants, such as data protection officers (DPOs) or managers of departments responsible for data processing. A semi-structured interview guide with open-ended questions shall be targeted to explore in-depth responses from key informants. The guide shall cover topics related to GDPR implementation, privacy practices, and challenges faced. This random interview could explore their experiences, challenges, and perceptions regarding GDPR compliance and privacy assurance.

7.2.3 Data analysis strategies

Quantitative Analysis: Alongside the mentioned methodologies, the data will also capture economic indicators of the software package implementation industry, such as its contribution to India's GDP. This will be vital in demonstrating the industry's significance in India's economy and hence the urgency in ensuring GDPR compliance. The collected data shall be analysed using Statistical tools (Ex : Minitab) covering descriptive statistics, regression analysis and statistical tests for proposed hypothesis.

Qualitative Analysis**:** We'll extract insights on GDPR's implications for the software package implementation industry in India, focusing on challenges, opportunities, and readiness for GDPR compliance, especially given its significant contribution to India's GDP. The information shall be collected in random on call interview to summarise qualitative interview data. Trend and thematic analysis shall be used to identify recurring themes and patterns in the responses. The data will be collated to review the themes related to GDPR compliance and privacy assurance.

8 Ethics and Human Subjects Issues

We plan to add a disclaimer in questionnaire as well as to inform the respondents about the confidentiality of their personnel data. If needed, we shall ask for their consent during online surveys and interviews or after in order to use the answers or data resulting from the questionnaires sent tosurvey

respondents and interview participants. In order protect the privacy and confidentiality of respondents, their immediate Personal identifiers (Ex: Full name, contact number, Organization, Mail id etc.,) shall not be disclosed and stored securely.

9 Key Strengths and Weaknesses of the Study

9.1 Key strengths

- Multidisciplinary approach combining IT, legal, and policy perspectives.
- In-depth analysis of GDPR challenges in the Indian data processor context.
- Proposing a new framework for GDPR compliance with local adaptations.
- Providing a clear link between the economic significance of the software package implementation industry in India and the need for GDPR compliance.
- Using real-world economic data to emphasize the importance of GDPR compliance for the industry.

9.2 Weaknesses/ constraints

- Reliance on self-reported data from the stakeholders of software Package organizations.
- Limited harmonization beyond the Indian software industry.
- Potential bias in responses due to self-interest.
- Confidentiality of information as many analyse companies will have difficulties to reveal the accurate information regarding the potential negative impacts on their profitability in case of non full or partial compliance with EU-GDPR standards.

10 Study Significance

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 importance of GDPR compliance 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 protection practices and ensuring the responsible use of personal data and its security aligned towards Compliance.

11 Limitations of the DPDP Act over EU-GDPR

While GDPR is designed to provide a high level of data protection and privacy, the DPDP Act, which represents a significant step for India in data protection and privacy standards, may have differences and potentially weaker aspects compared to GDPR. However, it's essential to consider that the DPDP Act is tailored to the Indian context and may evolve over time to align more closely with global standards.

A high-level summary of weaker aspects of the Digital Personal Data Protection Act in comparison to the EU General Data Protection Regulation (DR. Reeta, 2023) :

1. Fines and penalties

- DPDP Act imposes lower fines compared to GDPR. GDPR fines can go up to 4% of annual global turnover or €20 million Max, which ever is higher, while DPDP Act fines are limited to INR 15 Crore (approximately €1.75 million Max).

2. Data subject rights

- While 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.

3. Cross-border data transfer

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

4. Data breach notifications

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

5. Data protection officers (DPOs)

- GDPR mandates the appointment of Data Protection Officers (DPOs) in certain cases, ensuring expertise in data protection. DPDP Act has similar provisions but may not have as stringent requirements for DPOs.

6. Independent supervisory authority

- While GDPR establishes independent supervisory authorities in each EU member 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.

7. Consent requirements

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

8. Territorial scope

- GDPR has a broad territorial scope, applying to organizations outside the EU that process data of EU residents. DPDP Act primarily applies to data processing within India, potentially limiting its extraterritorial reach.

9. 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.

10. Enforcement and oversight

- While GDPR establishes well-defined roles for independent supervisory authorities, DPDP Act grants significant power to the Central Government, which may affect enforcement and oversight independence.

11. 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.

12. Concerns about data processing over privacy

- The DPDP Act has been criticized for seemingly prioritizing data processing over privacy protection, which contradicts the original intent of safeguarding individuals' rights and personal data.

Given these gaps and limitations, it becomes evident that there is a pressing need for a comprehensive and robust data protection framework in India, specifically tailored to the software package implementation industry and aligned more closely with globally recognized standards, such as the European Union's General Data Protection Regulation (EU-GDPR).

12 Conclusion

The GDPR has demonstrated its effectiveness in protecting individual privacy, providing clear guidelines for data processing, and ensuring transparency and accountability across the globe. Its stringent consent rules, data breach notification requirements, and emphasis on individual rights have become gold standards in the field of data protection.

The DPDP provides a good basis for Indian companies to be in compliance with legislation in India. In other words, the authors consider it as a second-best solution for Indian corporate world specialized in a very demanding industry which is a the software package implementation industry. This growing industry represents a significant part in Indian GDP, and a positive commercial balance due to exports and consequently many other positive aspects such as employment, consumption, production, investments, all contributing to GDP increase. However, due to many limitations of the DPDP, there is a clear need for further improvements of the DPDP which the authors believe that can be covered by using EU-GDPR as a first best solution.

By aligning with EU-GDPR principles, Act and create a more robust and internationally recognized data protection framework, especially relevant to the software package implementation industry, which serves EU clients. Such alignment would not only bolster data privacy but also enhance India's position in global data markets by instilling trust among EU businesses and organizations. This first best solution will make Indian companies more competitive and profitable as being compliant with market expectations can only help the Indian economy, and more specifically to the software package implementation industry.

Finally, from the analysed hypothesis the study will result in conclusion that the DPDP Act represents a progress in India's data protection landscape, but it is imperative to address its limitations within the context of establishing an EU-GDPR-based privacy assurance framework for Indian data processors in the software package implementation industry. Doing so will not only ensure data privacy within India but also guarantee compatibility with global data protection norms, strengthen commitment to data protection across borders, and foster trust in India's digital economy, particularly in its dealings with EU-based clients. There will be also a reflection if a mix of EU-GDPR standards with the DPDP is a best framework for the software package implementation industry in India where the balance would be made between the global expectation and local specificities. The research accentuates the link between the economic weight of the software package implementation industry in India and the imperative for GDPR compliance. A robust GDPR compliance framework is not just a legal necessity but an economic one, ensuring that India continues to maintain its significant GDP contribution from this industry while fostering global trust.

13 Tables

Table 1:Personal Data or Personally identifiable information (PII)

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

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

Table 2:Evolution of GDPR

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

Year	Milestone in the Evolution of GDPR
2009	The Lisbon Treaty, which entered into force, expanded the legal basis for data protection in the EU.
2012	The European Commission proposed a comprehensive reform of data protection laws to address new challenges posed by technological advancements.
2016	The European Union adopted the General Data Protection Regulation (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 (right to erasure), and mandatory data breach notifications.
2020	The European Data Protection Board (EDPB) was established to ensure consistent application of GDPR across the EU.
2021	The UK implemented its own version of GDPR known as the UK GDPR after Brexit.
2023 (Tentative)	Ongoing evolution and adaptation of GDPR to address emerging privacy challenges and technological advancements.

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

Table 3: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 unauthorized access to computer systems.
2011	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 were enacted, providing detailed guidelines for data protection.
2017	The Supreme Court of India declared the right to privacy as a fundamental right under the Indian Constitution.
2017	The Srikrishna Committee was formed to draft a comprehensive data protection law for India.
2018	Srikrishna Committee released the Personal Data Protection Bill (PDPB), which later evolved into the Data Protection Bill, 2019.

Year	Milestone in Data Privacy Regulation
2019	Data Protection Bill, 2019 was introduced in Parliament, setting the stage 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 Data Protection Bill, 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 independent regulatory body for data protection.
2022	The Data Protection Bill, 2022, incorporating changes based on public feedback, was introduced in Parliament.
2023	The Data Protection Bill (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, establishing a comprehensive data protection framework in India.

Source: (Gupta, 2020)

Table 4:Comparison of GDPR vs. DPDP

Aspect	GDPR	DPDP (Digital Personal Data Protection Act 2023)
Legal Basis	European Union Regulation	Indian Legislation
Applicability	European Union Member States	India
Extraterritorial Application	Yes, applies globally if processing EU residents' data	Yes, applies globally if offering goods or services to individuals 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	Up to 20 million EUR or 4% of global annual turnover	Up to 250 crores INR or 4% of global turnover, whichever is higher
Enforcement Authority	Various supervisory authorities for regions	Data Protection Board of India

Aspect	GDPR	DPDP (Digital Personal Data Protection Act 2023)
Data Localization Requirements (within country)	No – Covered in overall framework	Yes, sensitive personal data to be stored only in India

Source:(Chaturvedi and Sinha, 2017)

Table 5:GDPR vs. DPDP Fines

Violation Description	GDPR Fine (EUR)	DPDP Fine (INR)
Data breach with delayed notification	Up to 20 million or 4% of global annual turnover, whichever is higher	Up to ₹250 crores
Violation of data subject rights	Up to 20 million or 4% of global annual turnover, whichever is higher	Up to ₹200 crores
Non-compliance with GDPR principles and obligations	Up to 10 million or 2% of global annual turnover, whichever is higher	Up to ₹100 crores
Violation of consent and processing conditions	Up to 20 million or 4% of global annual turnover, whichever is higher	Up to ₹250 crores
Failure to cooperate with supervisory authorities	Up to 10 million or 2% of global annual turnover, whichever is higher	Up to ₹100 crores
Unauthorized international data transfers	Up to 20 million or 4% of global annual turnover, whichever is higher	Up to ₹250 crores
Lack of Data Protection Impact Assessment (DPIA)	Up to 10 million or 2% of global annual turnover, whichever is higher	Up to ₹100 crores
Inadequate data protection by design and by default	Up to 10 million or 2% of global annual turnover, whichever is higher	Up to ₹100 crores

Source :(Kuner, 2020)

Table 6: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

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
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
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 (projected)	8. Ensuring data ethics and responsible data handling	Ethical concerns, potential data misuse	Negative impact

Source:(Ministry of Statistics and Programme Implementation, 2021)

This structured table provides a clear view of how GDP growth in the Indian IT sector, data privacy importance, and the impact of not having GDPR and DPDP Act are related over the years.

References

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).

Ashraf, S. (2021) *GDPR Implementation Framework for SMEs*. Thesis Report. Metropolia University of Applied Sciences.

Available at: https://urn.fi/URN:NBN:fi:amk-202103314092 (Accessed: 1 November 2023).

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).

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).

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).

Falivene, L. and Falivene, L.I. (2021) *Understanding the Privacy Awareness Gap*. Thesis Report. Carnegie Mellon University.

Available at: https://www.researchgate.net/publication/354062996_Understanding_the_Privacy_Awareness_Gap (Accessed: 1 November 2023).

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).

Gartner (2022) *Gartner Forecasts India Application Software Spending to Grow 15% in 2022 - Blog*.

Available at: https://www.gartner.com/en/newsroom/press-releases/2022-08-24-india-software-spending-forecast (Accessed: 20 March 2023).

Gonzalez-Granadillo, G. *et al.* (2021) 'Automated Cyber and Privacy Risk Management Toolkit', *Sensors*, 21(16), p. 5493. doi:10.3390/s21165493.

Gupta, G. (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* [Preprint].

Available at: https://archives.palarch.nl/index.php/jae/article/view/3999/3938 (Accessed: 2 November 2023).

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).

Hrischev, R. (2020) 'ERP systems and data security', in *IOP Conference Series: Materials Science and Engineering*. Bulgaria: Institute of Physics Publishing. doi:10.1088/1757-899X/878/1/012009.

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).

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).

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

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

Lekhi, R. (2021) '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).

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.

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).

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).

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).

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.

(END OF DOCUMENT)