Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/22657
DOI URL: http://dx.doi.org/10.21474/IJAR01/22657

ISSN (O): 2320-5407
ISSN (P): 3107-4928

RESEARCH ARTICLE

FROM CONCEPT TO COMPLIANCE: PRIVACY BY DESIGN UNDER GDPR AND INDIA'S DATA PROTECTION LAWS

Raja Sengupta

1. General Counsel - TRDP Group, VCherish Labs

Manuscript Info

Manuscript History
Received: 12 November 2025
Final Accepted: 14 December 2025
Published: January 2026

Key words:-
"Privacy by Design," "Data Protection," "GDPR," "DPDPA," "Data PrivacyFrame work."

Abstract

Privacy by Design ("PbD") has evolved from a conceptual framework into a fundamental regulatory requirement, shaping data protection in the global digital economy. Developed in the early 1990s by Dr. Ann Cavoukian, PbD is now a key component of major privacy regulations, including the General Data Protection Regulation ("GDPR") in the EU and India's Digital Personal Data Protection Act("DPDPA"). This articl e focuses on the DPDPA, outlining its objectives, scope, and key provis ions related to PbD. It compares the Indian approach with the GDPR, highlighting similarities and differences in the regulatory frameworks and their implications for businesses. The analysis addresses how PbD principles are integrated into business practices and examines the challenges and opportunities faced in the dynamic digital landscape. The discussion underscores the critical role of PbD in modern data protection laws, emphasizing the need for proactive privacy measures. As regulations continue to evolve, businesses must embed privacy practices into their core operations to stay compliant. This shift from theory to practice reflects a broader trend towards ensuring robust data protection and responding to emerging privacy concerns. In conclusion, Privacy by Design stands as a cornerstone of contemporary data protect ion frameworks. Its integration into legal requirements like the GDPR and DPDPA highlights the importance of building privacy into the desi gn of products and services from the outset. Businesses that prioritize these principles will not only meet regulatory demands but also gain a competitive advantage in an increasingly privacy-conscious market.

Introduction:-

In our increasingly digital world, where personal data flows seamlessly across borders and platforms, Privacy by Design ("PbD") has become essential for safeguarding privacy. Developed by Ann Cavoukian in the early 1990s, PbD promotes embedding privacy measures into the design and operation of information systems from the outset. This proactive approach contrasts with the traditional reactive stance, where privacy concerns are addressed only after problems arise. The PbD framework mandates that privacy safeguards be seamlessly integrated into the operational phase of all activities and data processing, rather than being added as an afterthought following a

Corresponding Author:-Raja Sengupta
Adress:- General Counsel - TRDP Group, VCherish Labs

security incident or data breach. This approach ensures robust data privacy protections are maintained throughout the entire life cycle of a project or system.[1]The growing digital economy has underscored the importance of PbD. Businesses now collect, process, and analyze vast amounts of personal data, intensifying the need for robust privacy practices. Data breaches and privacy violations have become commonplace, highlighting the risks associated with inadequate data protection. PbD addresses these risks by integrating privacy considerations into the design and operation of systems, thus preventing potential issues before they arise.

Originally, PbD emerged from the recognition that privacy should be an integral part of technology and organizational practices, not a mere add-on. Cavoukian introduced PbD as a set of principles to proactively protect privacy throughout the lifecycle of information systems.[2] These principles include designing technologies with privacy in mind, ensuring that privacy measures are comprehensive rather than partial, and adopting a positive-sum approach where privacy enhancements support rather than hinder business goals. Over time, PbD has evolved from a theoretical concept into practical guidelines for organizations seeking to implement effective data protection measures. This evolution reflects a broader shift towards anticipatory privacy practices that address potential risks before they materialize.

As data protection regulations have become stricter, organizations have increasingly adopted PbD principles to ensure compliance and build stakeholder trust. The digital economy has transformed how businesses handle personal data, driving innovation, optimizing operations, and personalizing customer experiences. However, this data-centric approach also presents significant privacy challenges. The volume and sensitivity of data have increased, making strong privacy measures crucial for protecting personal information.

Legal frameworks like the General Data Protection Regulation ("GDPR") and India's Digital Personal Data Protection Act ("DPDPA" or the "Act") shape privacy practices in today's global digital economy. The GDPR, enacted by the European Union in 2018, sets a high standard for data protection and privacy. It requires organizations to integrate privacy considerations into their operations, ensuring compliance with strict privacy requirements. Similarly, the DPDPA, introduced in India in 2023, provides a comprehensive framework for data protection in the Indian context. While aligning with global standards, the DPDPA addresses specific local challenges, reflecting India's commitment to enhancing data protection and privacy.

Both the GDPR and DPDPA emphasize the importance of integrating privacy measures into data management practices, highlighting a global trend towards rigorous data protection standards. This article explores the evolution of PbD from a theoretical concept to a regulatory requirement under the GDPR and DPDPA. It examines how PbD principles are integrated within these frameworks and assesses their impact on businesses and consumers. By analyzing practical applications, the article demonstrates how organizations can effectively implement these principles to ensure compliance, build trust, and mitigate risks. The article also compares the specific requirements of the GDPR and DPDPA, explores the challenges organizations face in meeting these demands, and highlights the benefits of adopting a PbD approach, such as enhanced data protection, increased consumer trust, and alignment with global privacy standards.In summary, PbDrepresents a significant shift towards proactive and comprehensive data protection. As the digital economy expands and regulations like the GDPR and DPDPA set new standards for privacy, understanding and implementing PbD principles will be crucial for organizations aiming to protect personal data and build trust with stakeholders. This article provides a thorough analysis of the evolution, contextual relevance, and implications of PbD for businesses and consumers, offering valuable insights into this critical aspect of modern data protection.

Historical Context And Development Of Privacy By Design:-

Foundational Principles of Privacy by Design:-

As digital technologies rapidly advance, the safeguarding of personal data has emerged as a critical concern in our interconnected world. Amidst these advancements, Dr. Ann Cavoukian's pioneering concept of PbD has become a

[1] European Data Protection Supervisor, 'Preliminary Opinion on privacy by design – Opinion 5/2018' https://edps.europa.eu/sites/edp/files/publication/18-05 31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[2] Ann Cavoukian, Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, UC SANTA CRUZ, https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.

cornerstone of modern data protection practices. Originating in the early 1990s, PbD represents a proactive approach to privacy, integrating it into the very fabric of technology and business processes. This historical overview delved into the origins, evolution, and legal integration of PbD, highlighting its journey from a visionary idea to a fundamental requirement in global privacy regulations.[3]

In the early 1990s, as digital technology began reshaping how we interact with information, privacy concerns grew increasingly complex. Dr. Ann Cavoukian, then the Information and Privacy Commissioner of Ontario, recognized the limitations of reactive privacy measures, which often addressed privacy breaches only after they occurred. To address this gap, she introduced PbD—a concept designed to embed privacy considerations into the design of systems and processes from the outset. Dr. Cavoukian's framework was built on seven foundational principles aimed at ensuring privacy was not an afterthought but a core element of system design.[4] These principles include:

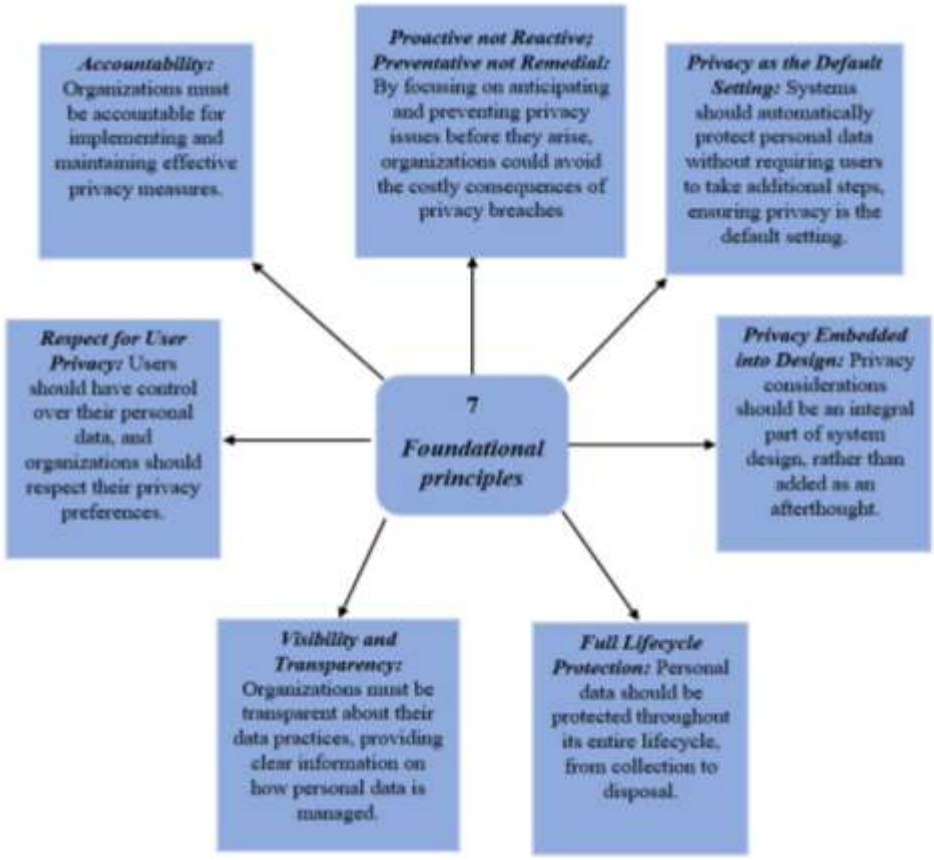

Figure 1 - The Seven Foundational Principles of Privacy by Design

These principles marked a paradigm shift in privacy management, advocating for a proactive approach that integrates privacy protections into technology and business practices from the start.

Evolution and Global Recognition:-

The concept of PbD gained momentum over the years, evolving from a best practice to a globally recognized standard. Initially, Dr. Cavoukian's advocacy and the framework's adoption by privacy professionals set the stage for broader recognition.

[3] Office of the Information and Privacy Commissioner, Ontario, Canada, Annual Report (2012), https://www.ipc.on.ca/sites/default/files/legacy/Resources/ar-2012-e.pdf

[4] Ann Cavoukian, Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers, GPS, (2011), https://gpsbydesigncentre.com/wp-content/uploads/2022/02/312239.pdf.

Early Adoption (1990s-2000s):
During the late 1990s and early 2000s, Dr. Cavoukian's work garnered attention from privacy advocates and organizations. This period saw the dissemination of PbD principles through various conferences and publications, laying the groundwork for its broader adoption.

International Endorsement (2000s-2010s):-
As data privacy concerns intensified globally, PbD principles gained formal recognition from international privacy organizations. Notably, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2002)[5] and the International Conference of Data Protection and Privacy Commissioners (now known as the Global Privacy Assembly) included PbD in their recommendations.[6] The OECD guidelines endorsed the concept of embedding privacy into the design of systems as a proactive measure to enhance data protection.

Integration into Legal Frameworks (2010s):-
The most notable milestone in the evolution of Privacy by Design (PbD) was its inclusion in the European Union's GDPR, adopted in 2016 and enforced from May 2018. The GDPR mandates that organizations implement "technical and organizational measures" at the earliest stages of designing processing operations to ensure that privacy and data protection principles are embedded from the start—reflecting the concept of PbD. Additionally, by default, companies must ensure that personal data is processed with the highest level of privacy protection. This means only the necessary data should be processed, with minimal storage periods and limited accessibility, ensuring that personal data is not automatically accessible to an indefinite number of individuals—known as "data protection by default."[7] This integration of PbD into the GDPR reflects its elevated status as a proactive and legally required approach in global data protection practices.

Influence on Global Privacy Regulations (2010s-Present):-
The inclusion of PbD principles in the GDPR has inspired other jurisdictions to update their privacy regulations. For instance, Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") was updated to include PbD principles, as seen in the PIPEDA Reform Document[8]. Similarly, the California Consumer Privacy Act ("CCPA") incorporates PbD principles into its framework, emphasizing privacy considerations at every stage of data processing.[9] CCPA is a significant example of this trend.While Canadian and Californian regulators encourage privacy-by-design, neither PIPEDA nor the CCPA contains a statutory obligation equivalent to Article 25 of the GDPR. PIPEDA's reform proposals and industry guidance recommend embedding privacy in system design, but no binding duty has yet been enacted. Similarly, the CCPA emphasises notice and opt-out rights and requires "reasonable security," but does not impose a legally binding privacy-by-default requirement. Clarifying this distinction avoids implying that these regimes codify Design by Default. Further, the Association of Southeast Asian Nations ("ASEAN") has recognized the importance of integrating PbD principles into its data governance policies. The ASEAN Data Management Framework reflects this by embedding data protection and governance measures throughout the entire data lifecycle, ensuring that privacy safeguards are in place from the outset.[10] This initiative demonstrates ASEAN's commitment to proactive data protection strategies in line with global best practices.

Ongoing Recognition and Endorsement (Present):-

[5]OECD (2002), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris, https://doi.org/10.1787/9789264196391-en.
[6] International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design (Oct. 27-29, 2010), https://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf.
[7] European Commission, What does data protection 'by design' and 'by default' mean?, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en, (last visited Sept. 16, 2024)
[8] Office of the Privacy Commissioner of Canada, 2018-2019 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act (2009), https://www.priv.gc.ca/media/5076/ar_201819_eng.pdf.
[9] California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100-1798.199 (2020).
[10]ASEAN, ASEAN Data Management Framework (2021), https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf.

Today, PbD remains a cornerstone of modern data protection practices. Leading privacy organizations, such as the International Association of Privacy Professionals ("IAPP")[11], and the International Institute of Communications ("IIC"), continue to promote PbD as an essential component of effective data protection strategies. The ongoing endorsement of PbD underscores its critical role in shaping privacy standards and ensuring that privacy considerations are deeply embedded in the development of new technologies and services.

Privacy by Designas a Legal Requirement:-
The transition of PbDfrom a conceptual framework to a legal requirement emphasizes its importance in modern privacy regulation. This shift is evident in the integration of PbD principles into major privacy laws such as the GDPR and India's DPDPA.

Privacy by Design under the GDPR:-
GDPR represents a significant advancement in privacy law, particularly through its integration of PbD as a mandatory requirement. This regulation, which came into effect on May 25, 2018, underlines the European Union's commitment to upholding privacy and data protection standards. The GDPR is codified as Regulation (EU) 2016/679, and its comprehensive approach reflects a robust legal framework for data protection.

Designing Privacy into Systems:-
Article 25 of the GDPR, titled "Data Protection by Design and by Default ("DPbDD"),"establishes the principle that privacy should be incorporated into the design of systems and processes from the outset. This article stipulates:

- Article 25(1): "Taking into account the state of the art, the cost of implementation and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement the data protection principles effectively and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."[12]

- Article 25(2): "The controller shall implement appropriate measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility."[13]

Furthermore, according to Recital 78 of the GDPR, organizations involved in developing, designing, selecting, and using applications, services, and products that rely on the processing of personal data are encouraged to prioritize data protection by implementing DPbDDprinciples. Consequently, to meet their data protection obligations, controllers should select and utilize applications, services, and products that inherently incorporate these DPbDDrequirements in their data processing activities.[14]The GDPR mandates that organizations design their data processing systems to ensure data protection principles are effectively integrated, considering the latest technological developments, the costs of implementation, and the specific risks associated with data processing.

Conducting Data Protection Impact Assessments (DPIAs):-
Article 35 of the GDPR[15] requires organizations to conduct Data Protection Impact Assessments ("DPIAs") when processing activities are likely to result in high risks to the rights and freedoms of individuals. This article outlines:

- **Article 35(1):** "When a type of processing in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms

[11] R. Jason Cronk, Strategic Privacy by Design, (The International Association of Privacy Professionals, 2nded. 2022).
[12]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)2016, L 119, art. 25 ¶ 1,https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[13]Id.
[14]Id. at 15.
[15]Id.at 53.

of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

- **Article 35(7):** "The assessment referred to in paragraph 1 shall be carried out prior to the processing and shall, in particular, assess the necessity and proportionality of the processing operations in relation to their purpose, assess the risks to the rights and freedoms of data subjects, and mitigate the risks identified."

DPIAs play a crucial role in identifying and mitigating privacy risks before data processing begins. They ensure that potential issues are addressed proactively, helping organizations comply with GDPR requirements and protect individuals' rights.

Implementing Data Minimization:-
Article 5 of the GDPR enshrines the principle of data minimization, which requires organizations to limit data collection and processing to what is necessary for the intended purpose. This principle is articulated in:

- **Article 5(1)(c):**"Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')."[16]

Data minimization ensures that organizations only collect and process the minimum amount of personal data required for their specific purposes, thereby reducing the risk of unnecessary data exposure.

Ensuring Transparency and Accountability:-
Article 12 of the GDPR focuses on transparency, while Articles 24 and 28 emphasize accountability. Key provisions include:

- **Article 12(1):**"The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language."[17]

- **Article 24(1):**"Taking into account the state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation…"[18]

- **Article 28(1):**"Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."[19]

  These articles ensure that organizations maintain transparency in their data practices and are accountable for implementing effective privacy measures, thereby reinforcing trust and compliance with GDPR requirements.

Privacy by Design (PbD) under the DPDPA:-
India's DPDPA, enacted in 2023, follows a similar trajectory to the GDPR in integrating privacy by design principles into its regulatory framework. The DPDPA represents India's comprehensive effort to align its data protection standards with global best practices.

Designing for Privacy:-
Section 8 of the DPDPA emphasizes the integration of privacy considerations into system design. The section states:

[16]Id.at 35.
[17]Id.at 39.
[18]Id. at 47.
[19]Id. at 49.

- **Section 8(4):**"A Data Fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act and the rules made thereunder."[20]

- **Section 8(5):** "A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach."[21]

The Act requires that a Data Fiduciary implement robust technical and organizational measures, in line with the privacy by design concept, to ensure compliance with data protection provisions and to safeguard personal data through proactive security safeguards to prevent breaches.

Conducting Impact Assessments:-
Section 10 of the DPDPA requires data fiduciaries to conduct impact assessments similar to GDPR's DPIAs.

The section outlines:
- **Section 10(2)(c)(i):** "periodic Data Protection Impact Assessment, which shall be a process comprising a description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals, and such other matters regarding such process as may be prescribed;"[22]

The requirement for impact assessments ensures that organizations proactively address privacy risks and enhance data protection measures.

Minimizing Data Collection:-
Although the DPDPA does not articulate a standalone data-minimisation principle, minimisation can be inferred from Section 8(4) and the DPDP Rules 2025. Section 8(4) requires data fiduciaries to implement appropriate technical and organisational measures, while Rule 8 mandates erasure of personal data once the specified purpose has been served (with prescribed retention periods). These provisions encourage organisations to limit the collection and retention of data to what is necessary for the intended purpose.[23]This provision ensures that organizations limit their data collection and processing to what is strictly necessary, reducing the risk of excessive data handling.

Transparency and Accountability:-
Sections 4, 6, and 8 of the DPDPA mandate that personal data processing must be conducted in accordance with the law, with a lawful purpose, and must meet transparency requirements during consent collection.[24] Data fiduciaries are accountable for their processors' activities and must ensure compliance by publishing the contact details of their Data Protection Officer ("DPO") or a designated individual to address data protection inquiries.[25] Additionally, organizations are required to establish a grievance redressal mechanism to enable data principals to file complaints.[26]These provisions ensure that organizations are transparent about their data practices and accountable for maintaining effective privacy measures, fostering trust and compliance.The integration of PbD into regulatory frameworks such as the GDPR and India's DPDPA reflects a global commitment to proactive data protection. Both the GDPR and the DPDPA mandate organizations to embed privacy into the design of systems and processes, conduct impact assessments, minimize data collection, and ensure transparency and accountability.

By adopting these principles, organizations can better safeguard personal data, comply with regulatory requirements, and build trust with stakeholders in an increasingly data-driven world. The evolution of PbD from a conceptual framework to a legal requirement underscores its critical role in modern privacy practices and highlights the ongoing importance of proactive data protection in safeguarding individuals' rights.

[20]Digital Personal Data Protection Act, No. 22 of 2023, § 8 (Ind.), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
[21]Id.
[22]Id. § 10 (Ind.).
[23]Id., § 7 (Ind.)
[24]Id., § 4(1) (Ind.)
[25]Id., § 6(3) (Ind.)
[26]Id., § 8(10) (Ind.)

The General Data Protection Regulation:-

Overview of GDPR:-

The GDPR is a landmark in data protection law, fundamentally reshaping how organizations manage personal data across Europe. Enacted by the European Union and effective from May 25, 2018, GDPR, formally known as Regulation (EU) 2016/679, seeks to harmonize data protection laws within the EU, strengthen individual privacy rights, and establish a robust framework for data security. The regulation addresses the rapid growth of digital technology and the escalating significance of personal data in the global economy. The core objectives of the GDPR include as follows:

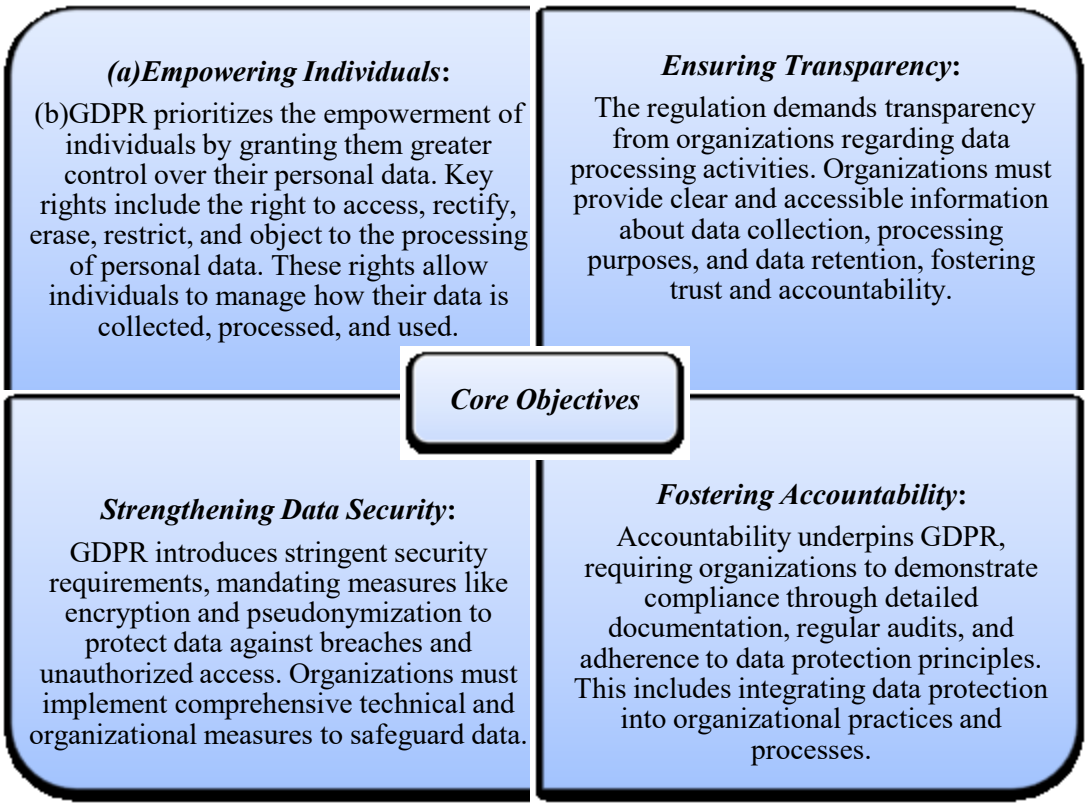

Figure 2 – Core Objectives of the GDPR

Key Provisions:

Data protection principles:

Article 5 of the General Data Protection Regulation (GDPR) outlines fundamental principles central to data protection compliance. These principles not only underpin the GDPR but also shape the various rules and obligations within the legislation. Adhering to these principles is essential for controllers to meet their GDPR obligations. Here's a summary of the Principles of Data Protection as defined in Article 5 GDPR[27]:

[27] See supra note 12, at 35-36

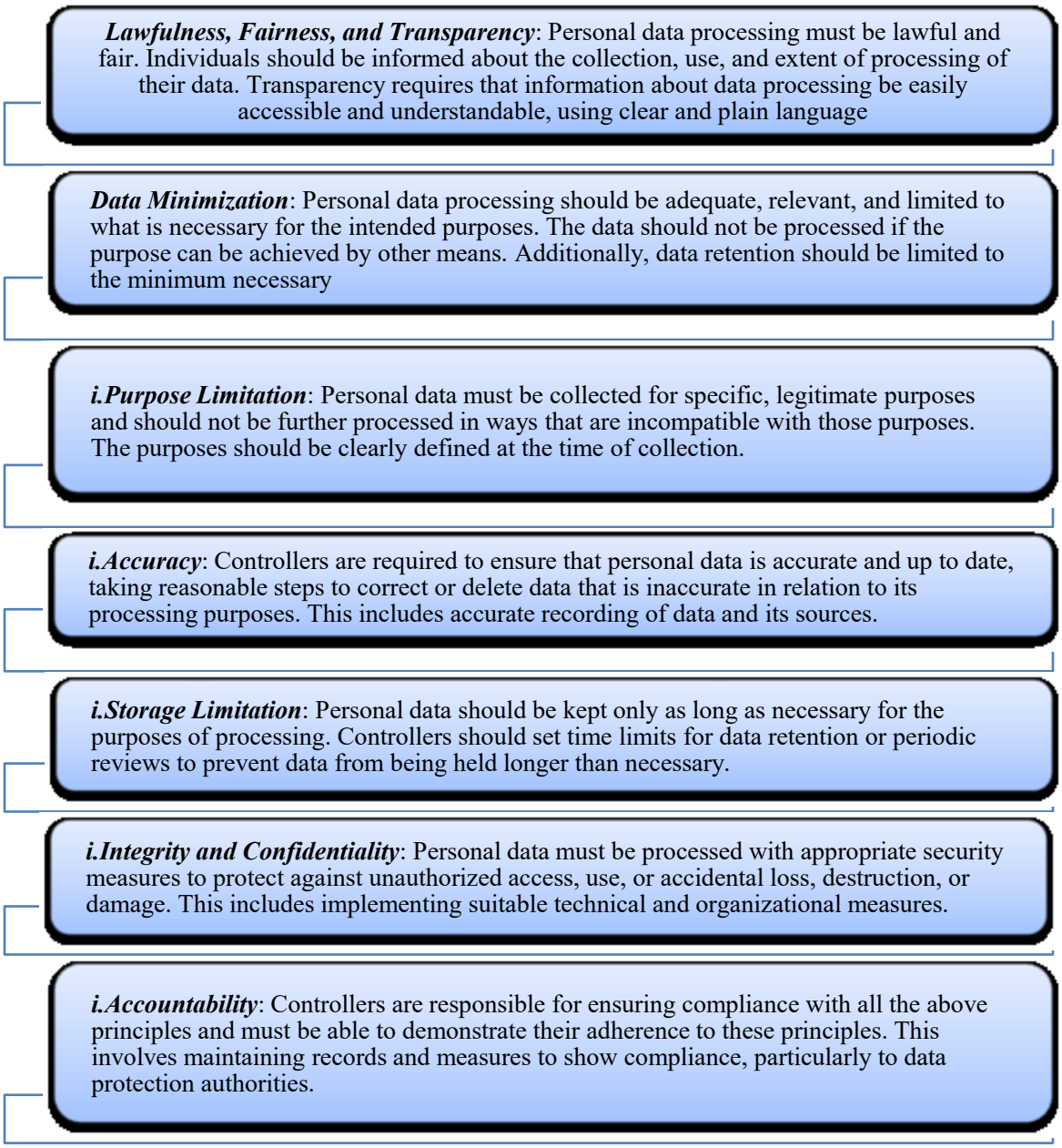

Figure 3 – Data protection principles
These principles serve as the foundation for ensuring effective data protection under the GDPR.

Lawfulness of processing:
The lawful bases for processing personal data, as outlined in Article 6 of the GDPR, include the following[28]:

[28] See supra note 12, at 36

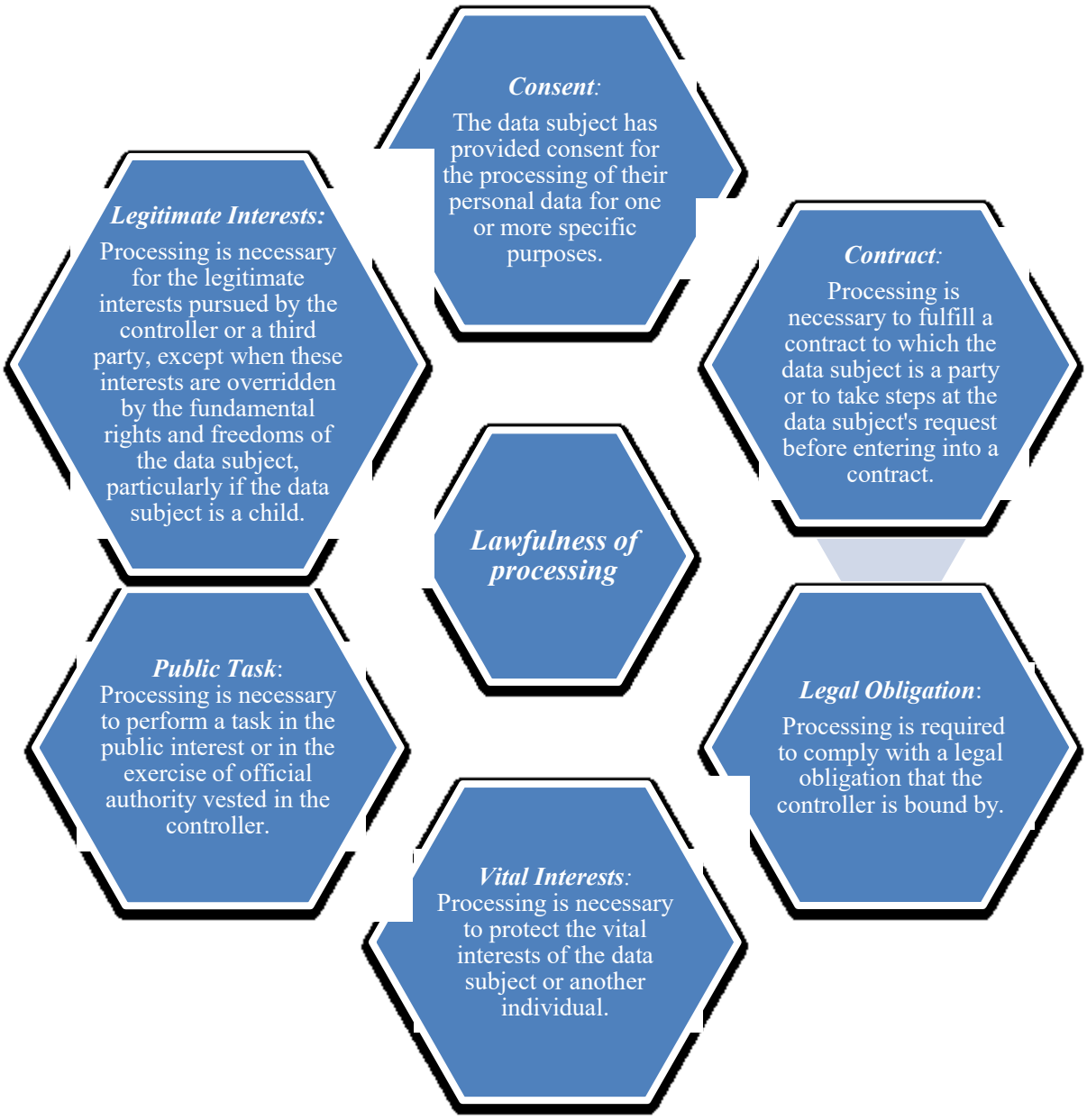

Figure 4 – Lawfulness of processing

Data subject rights:

The eight data subject rights established by the GDPR aim to empower individuals, enhance privacy protections, and ensure transparency and control over their personal data in the digital landscape.Some rights were introduced by earlier legislation[29] (such as the right to access) and further enhanced by GDPR, while others, like data portability, are new to GDPR.The GDPR provides the following eight rights for data subjects:

The right to be informed: The right to be informed allows individuals (data subjects) to access information about how their personal data is processed.

[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995, L 281, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

The organization (data controller) responsible for collecting and processing personal data must provide specific details about their data processing activities, including:

- The organization's information and contact details. (Article 13(1)(a))[30]
- The purpose of data processing. Article 13(1)(c)[31]
- The legal basis for processing personal data. Article 13(1)(d)[32]
- Details of third parties with whom data is shared. Article 13(1)(e)[33]
- The data retention period. Article 13(2)(a)[34]
- The right to file a complaint. Article 13(2)(d)[35]
- Whether providing personal data is a statutory or contractual requirement as well as Whether the data subject is obliged to provide their personal data. Article 13(2)(e)[36]
- This information must be provided in a concise, transparent, intelligible, and easily accessible manner, using clear and plain language.[37]

The right of access:

Article 15 of the GDPR grants individuals (data subjects) the right to access information about their personal data processed by an organization (data controller).

Specifically, data subjects can request details about[38]:

- The purpose of data processing.
- The categories of personal data processed, including recipients or categories of recipients in third countries or international organizations.
- The recipients to whom the personal data has been or will be disclosed.
- The retention period for storing the data.
- Request the erasure of their personal data.
- Ask for a restriction on the processing of their personal data.
- Request rectification of inaccurate data.
- Confirm whether the organization processes their personal data.
- Know the source of collected data.
- Be informed about the existence of automated decision-making and its effects on them.

When transferring personal data to a third country or an international organization, the data subject has the right to be informed about the appropriate safeguards for the transfer as outlined in Article 46, in accordance with Article 15(2) of the GDPR.[39]These rights ensure that individuals understand how their data is used and verify the lawfulness of data processing.

The right to rectification[40]:

Article 16 of the GDPR grants individuals (data subjects) the right to request the correction of inaccurate personal data from the organization (data controller) without undue delay. They can also request the completion of incomplete personal data. When an organization receives a rectification request, it must take several steps to address it. This includes verifying the accuracy of the data in question and, if necessary, halting the processing of the potentially incorrect data until verification is complete. Operationalizing this right can present challenges, as rectifying data may impact multiple data platforms within the organization.

[30]See supra note 12, at 40
[31] See supra note 12, at 40
[32] See supra note 12, at 41
[33] See supra note 12, at 41
[34] See supra note 12, at 41
[35] See supra note 12, at 41
[36] See supra note 12, at 41
[37] See supra note 17.
[38] See supra note 12, at 43
[39] See supra note 12, at 43
[40] See supra note 12, at 43

The right to erasure ('right to be forgotten'):
Article 17 of the GDPR[41] grants individuals (data subjects) the right to request the deletion of their personal data from an organization (data controller). This right, known as the right to be forgotten or the right to erasure, allows individuals to seek the removal of their personal data under certain conditions.

In the landmark case Google Spain and Google C-131/12[42], the Court of Justice of the European Union ("CJEU") established the "right to be forgotten," fundamentally reshaping data privacy laws in the EU. The case was brought by Mario Costeja González, who challenged Google Spain and Google Inc. over the display of outdated or irrelevant personal information in search engine results. The CJEU ruled that individuals have the right to request the removal of such data from search results under specific conditions. This decision emphasized that data controllers must implement robust privacy protections and integrate mechanisms for individuals to manage the visibility and accuracy of their personal data, aligning with the GDPR's principles of data minimization and user rights.

In another case Google v CNIL (C-507/17)[43], the Court of Justice of the European Union addressed the territorial scope of the right to be forgotten, establishing that de-referencing should generally apply EU-wide. This means search engines must take measures to prevent or significantly discourage access to de-referenced results from within the EU. However, this ruling allows non-EU countries to determine their own balance between data protection and freedom of information. The decision reflects the Court's effort to reconcile the conflicting rights and interests of the parties involved, often placing a greater emphasis on the right to data protection.

The right to restrict processing: Article 18 of the GDPR[44] grants individuals (data subjects) the right to restrict processing, allowing them to request a limitation on the processing of their personal data.

This right is often exercised as an alternative to requesting the deletion of the data.However, since this right is not absolute, it only applies in specific circumstances:
- The individual contests the accuracy of the data, and its accuracy is under verification.
- The processing is unlawful, but the data subject prefers to restrict its use rather than have the data erased (distinct from the right to erasure).
- The organization no longer requires the data for its original purpose, but the individual needs it preserved for legal claims.
- The organization is in the process of verifying a data erasure request.

From an operational standpoint, Recital 67 of the GDPR[45] provides guidance to organizations on methods to restrict processing, which may include:
- Temporarily moving the selected data to a different processing system.
- Making the selected personal data inaccessible to users.
- Temporarily removing published data from a website.

The right to data portability:
Article 20 of the GDPR[46] grants the right to data portability, enabling individuals (data subjects) to request and receive their personal data, which they have previously provided to an organization (data controller), in a structured, commonly used, and machine-readable format.

[41] See supra note 12, at 43-44
[42]Case C-131/12, Google Spain SL & Google Inc. v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González, 2014, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (last visited Sep. 06, 2024).
[43] Case C-507/17, Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), 2019, available athttps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0507(last visited Sep. 10, 2024).
[44]See supra note 12, at 44
[45] See supra note 12, at 13
[46] See supra note 12, at 45

This right empowers individuals to transfer their data across different services for their own purposes.Upon request, the organization can either send the data directly to the individual or transfer it to a recipient of the individual's choice.

This right applies only to data that the individual has directly provided to the organization, and only under specific conditions:

- the processing must be based on the individual's consent or related to the performance of a contract, and
- it must be carried out by automated means (excluding paper files).

The GDPR does not clearly define what constitutes a structured, commonly used, and machine-readable format, which poses challenges for organizations as they seek to update their IT systems and procedures to ensure compliance.However, Recital 68 of the GDPR[47] encourages data controllers to develop interoperable formats that facilitate data portability.

The right to object:

Article 21 of the GDPR[48] grants individuals (data subjects) the right to object to the processing of their personal data by an organization (data controller). This right allows individuals to request the cessation of processing activities under specific conditions.To exercise this right, individuals may submit their objection in writing or verbally, with a required explanation.The right to object is applicable in the following situations:

- When processing is based on legitimate interests or the performance of a task carried out in the public interest or in the exercise of official authority.
- When processing is conducted for direct marketing purposes.

The organization is not required to stop processing if it can demonstrate compelling legitimate grounds that override the interests and rights of the individual or if the processing is necessary for the establishment, exercise, or defense of legal claims.

Rights in relation to automated decision-making and profiling:

Article 22 of the GDPR[49] protects individuals (data subjects) from decisions based solely on automated processing and profiling that significantly affect them.This right is closely related to the right to object to data processing.The data controller must:

- provide individuals with information about the automated processing,
- offer a straightforward mechanism for data subjects to request human intervention or contest the decision, and
- conduct regular reviews of the automated decision-making system.

Automated decision-making that involves processing personal data is permitted under the following conditions:

- the processing is authorized by law,
- it is necessary for the performance of a contract, or the individual has given explicit consent.
-

A recent ruling by the European Court of Justice ("ECJ") in January 2023 further underscores the significance of these rights. In the case of Österreichische Post AG (Case C-154/21)[50], the ECJ clarified that under Article 15(1)(c) of the GDPR, data subjects have the right to know the specific identities of the recipients of their personal data, not just the categories of recipients. This decision emphasizes that data controllers must disclose the actual identities of data recipients upon request, reinforcing the right of access as essential for enabling data subjects to fully exercise their GDPR rights, including rectification, erasure, restriction of processing, and objection. By setting out these comprehensive rights, the GDPR ensures that individuals have robust control over their personal data, fostering trust and accountability in the digital age.

[47] See supra note 12, at 13
[48] See supra note 12, at 45-46
[49] See supra note 12, at 46
[50] Case C-154/21, RW v Österreichische Post AG, 2023, available at https://curia.europa.eu/juris/document/document.jsf?docid=269146&doclang=en (last visited Sep. 06, 2024).

In conclusion, the eight data subject rights established by the GDPR are instrumental in empowering individuals, enhancing privacy protections, and ensuring transparency in the handling of personal data. These rights collectively address key aspects of data processing—from providing clear information about data use and granting access to personal data, to enabling correction, erasure, and restriction of data. The GDPR's framework not only upholds fundamental privacy principles but also introduces innovative concepts such as data portability and safeguards against automated decision-making.

Integration of DPbDDin GDPR

DPbDD is a core principle of the GDPR, mandated under Article 25.[51]DPbDDshifts data protection from being a reactive measure to a proactive strategy, ensuring that privacy considerations are built into the design and operation of systems and processes from the outset.DPbDDare foundational principles in EU data protection regulatory frameworks. Compliance with these principles is a crucial legal requirement for any organization involved in the collection, storage, and processing of users' personal data. These approaches to data privacy are enshrined in the GDPR and have significantly influenced data protection laws worldwide.[52]

Article 25(1) - Data Protection by Design:

Article 25(1)[53] mandates that organizations (the controller) integrate data protection principles into system and process design:

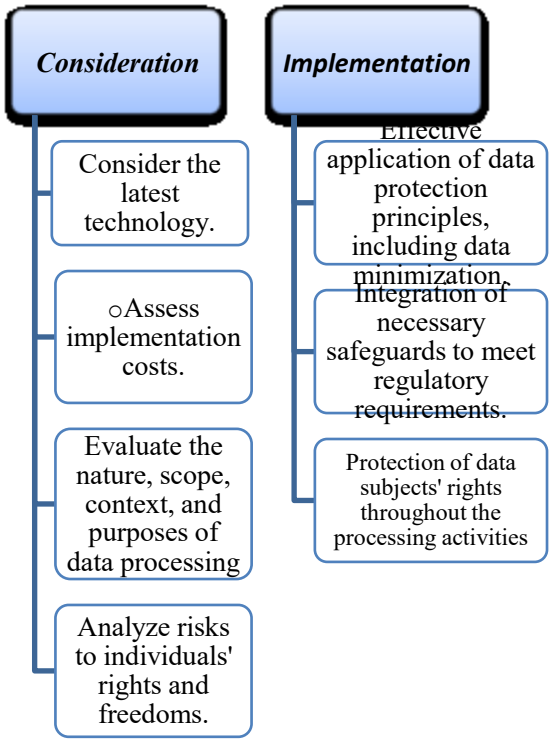

Figure 5 – Model Data Protection by Design Conceptual Framework

Article 25(2) - Data Protection by Default:

Article 25(2) requires organizations to ensure data protection by default.[54]To successfully implement a privacy-by-default approach, organizations must adhere to the following key measures[55]:

[51] See supra note 12, at 48

[52] European Data Protection Board, 'Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default' v 2.0 (20 October 2020),https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[53] See supra note 12.

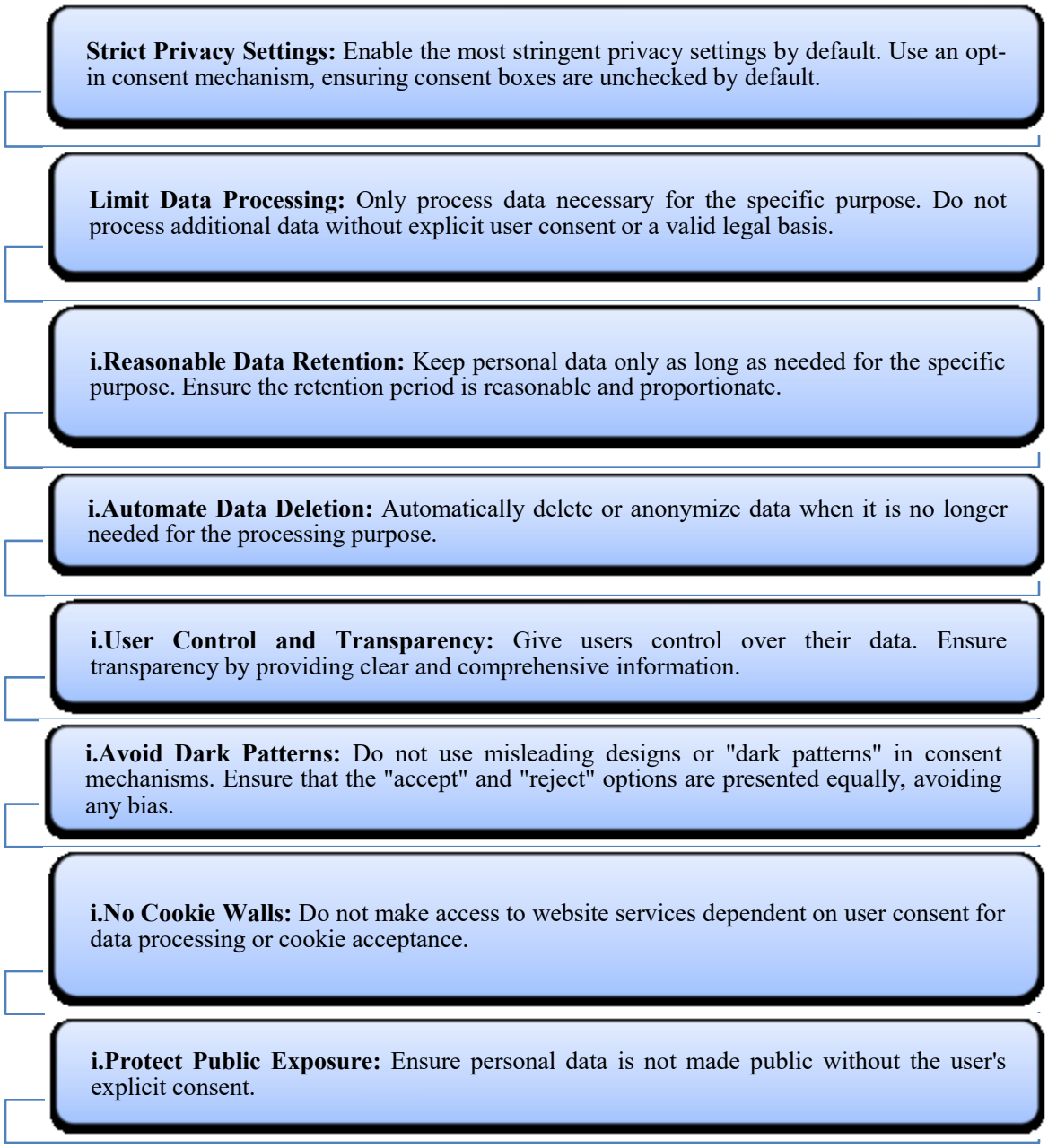

Figure 6 – Model Data Protection by Default Conceptual Framework

Data Protection by Design and by DefaultCertification:
Article 25(3) stipulates that certification in accordance with Article 42 can serve as evidence of compliance with DPbDD.[56] Conversely, documents demonstrating adherence to DPbDD principles can also be advantageous in the certification process.[57] This means that if a processing operation by a controller or processor is certified under Article 42, supervisory authorities should factor this certification into their assessment of GDPR compliance with

[54] See supra note 13.
[55] Data Consent Automation [Online],available at: https://securiti.ai/blog/privacy-by-design-privacy-by-default/.
[56] See supra note 47.
[57] See supra note 12, at 47.

respect to DPbDD.Certification according to Article 42[58] involves evaluating design processes, including the determination of processing methods, governance structures, and the technical and organizational measures necessary to enforce data protection principles.As per Article 42(5), certification criteria are set by certification bodies or scheme owners and must be approved by the competent supervisory authorityor the European Data Protection Board ("EDPB").[59] Despite obtaining certification under Article 42, the controller remains responsible for the ongoing monitoring and enhancement of compliance with the DPbDD requirements specified in Article 25.

In conclusion, embedding DPbDDinto data protection regulations signifies a crucial shift toward proactiveprivacy management. By integrating privacy considerations into the design and operational processes from the outset and ensuring that privacy is the default setting, organizations are better equipped to protect personal data. While certification can demonstrate compliance with these principles, continuous vigilance and improvement in privacy practices are essential. This integration underscores the importance of making privacy a foundational element of data protection and sets a global benchmark for effective privacy management.

Practical Implications for Organizations:-

Impact on Businesses:-

The integration of DPbDDunder GDPR drives significant changes in how organizations approach data protection, impacting various operational aspects.To comply with the DPbDDframework, organizations may adopt data-oriented or process-oriented strategies.[60]

Designing for Privacy:

Organizations must prioritize privacy by embedding privacy features into systems and processes right from the outset. This proactive approach involves several key strategies:

Conducting Privacy Impact Assessments ("PIAs"):

To ensure privacy is integrated into new projects or systems, organizations must conduct PIAs. These assessments help identify and address potential privacy risks early in the design process.

Example:

Before launching a new mobile app, Company A Inc. conducted a Privacy Impact Assessment to evaluate the potential impact of the app's features on user privacy. The assessment uncovered that the app is configured to request extensive location data, which is not essential for the app's core functionalities such as user engagement and content delivery.
Based on the assessment findings, Company A Inc. revised the app's design to restrict location data collection. The app is updated to request location access only when users' opt-in for features that genuinely require it, such as location-based recommendations or services. This redesign ensures that unnecessary data is not collected, thereby enhancing user privacy and aligning with privacy best practices.

Implementing Privacy by Default:

Privacy by Default means configuring systems and services to protect user privacy without requiring users to change settings. By default, users should be opted into the most privacy-friendly settings.

Example:

Company WApp Inc., a messaging app provider, is finalizing its product release. The app's current default settings do not include end-to-end encryption, and users must manually activate this feature to ensure the security of their conversations. This configuration could lead to potential vulnerabilities if users forget or choose not to enable encryption.

[58] See supra note 9, at 58

[59] See supra note 9, at 59.

[60] Jaap-Henk Hoepman, Privacy Design Strategies (The Little Blue Book) (19 April 2022),https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf.

In adherence to the principle of Privacy by Default, Company redesigned the app to integrate end-to-end encryption as the default setting for all user communications. This means that encryption is automatically enabled upon account creation, and all messages are securely encrypted without requiring users to manually adjust any settings. Additionally, the app now provides clear information about the encryption feature and its benefits during the onboarding process, ensuring users are aware of the default privacy protections. This approach safeguards user conversations by default and aligns with best practices for user privacy and security.

Conducting Data Protection Impact Assessments (DPIAs):
DPIAs are crucial for evaluating privacy risks in data processing activities. They help organizations identify, assess, and mitigate privacy risks, ensuring compliance with GDPR.

(a) Identifying Risks: Organizations must evaluate the risks associated with data processing activities and understand how these risks could impact individuals' privacy.

(b) Mitigating Risks: Once risks are identified, organizations must implement measures to mitigate them. This could involve modifying data processing practices or enhancing security measures.

Example:

A healthcare provider is in the process of developing a new patient data management system and conducts a Data Protection Impact Assessment to identify potential risks. The assessment uncovers several concerns: unauthorized access to sensitive health information due to inadequate role-based access controls, vulnerabilities in data transmission channels that could lead to data breaches, and risks associated with third-party integrations that may lack robust security measures.

To address these risks, the healthcare provider implemented a series of corrective actions.
First, they enhanced role-based access controls by introducing granular permissions and conducting regular access reviews to ensure that only authorized personnel can access sensitive data.
Second, they strengthened data encryption by applying advanced protocols, to protect data both at rest and during transmission.
Finally, they performed rigorous security assessments and compliance checks on all third-party services integrated with the system to ensure they adhere to stringent security standards.
These measures are designed to mitigate the identified risks and safeguard patient privacy effectively.

Implementing Data Minimization: Data Minimization is a key principle of GDPR, requiring organizations to collect only the data necessary for a specific purpose. This minimizes the risk of unnecessary data exposure.

Reviewing Collection Practices:
Organizations should regularly review their data collection practices to ensure they are aligned with the principle of data minimization. This includes evaluating whether the data being collected is truly necessary for the intended purpose.

Example:

A retail chain is evaluating its data collection practices to ensure compliance with the principle of data minimization. During a routine review, the company discovers that its customer loyalty program collects a wide range of personal information, including customers' social security numbers. The review reveals that this information is not necessary for the program's primary function of tracking purchase history and rewarding customer loyalty.

In response to this finding, the retail chain revised its data collection practices by removing the requirement for social security numbers from the loyalty program registration process. Instead, the company focuses on collecting only the data essential for the program's core functions, such as purchase history and customer preferences. This adjustment not only simplifies the data

collection process but also enhances customer privacy by ensuring that only necessary information is collected and retained.

Restricting Data Access:
Data access should be limited to individuals who need the information to perform their job functions. This reduces the risk of data breaches or unauthorized use of personal data.

Example:

A large law firm is reviewing its data access policies and discovers that sensitive client information, including case details and legal documents, is accessible to a broad range of employees across various departments. This widespread access poses a risk of unauthorized use or potential data breaches.

To enhance data security, the law firm implemented a restricted access policy where access to sensitive client information is limited to employees directly involved in handling those specific cases, such as lead attorneys and paralegals working on the case. Administrative staff and employees in unrelated departments are granted access only to non-sensitive information necessary for their job functions. This targeted approach ensures that sensitive data is protected from unauthorized access, thereby reducing the risk of data breaches and misuse.

Enhancing Transparency:
Transparency is a fundamental requirement under GDPR. Organizations must clearly communicate their data processing practices to users, ensuring that they understand how their data is being used.

Updating Privacy Notices:
Organizations must provide clear, accessible, and up-to-date privacy notices that explain their data processing practices in simple terms. These notices should be easy for users to find and understand.

Example:

A national utility company is preparing to update its customer management system. During this process, it realizes that its existing privacy notice does not effectively communicate how customer data is collected, used, or shared. The notice is written in complex legal jargon and is not easily accessible from the company's main website.

To address these issues, the utility company overhauls its privacy notice to ensure it is clear, accessible, and up-to-date. The updated notice is written in plain language, making it easy for customers to understand how their data is collected, used, and shared. It also includes specific details about data retention periods and the company's data protection measures. The revised notice is prominently displayed on the company's homepage and is accessible through multiple touchpoints, such as account management pages and customer service sections. This approach ensures that customers are well-informed about their privacy rights and how their data is handled.

Implementing Consent Mechanisms:
Obtaining and managing user consent is essential for lawful data processing. Organizations must develop mechanisms that allow users to give, withdraw, or manage their consent easily.

Example:

A large travel agency is launching a new, comprehensive customer loyalty program that includes personalized travel offers, targeted promotions, and dynamic pricing based on user preferences and behavior. The program aims to collect and analyze extensive data on customer travel habits, preferences, and purchase history. However, the current system lacks an effective consent mechanism for managing user preferences regarding data sharing and personalized content.

To address this, the travel agency developed a user-friendly consent management system as part of the loyalty program. Customers are provided with a straightforward interface where they can

easily opt in or out of data sharing for personalized offers. The system allows users to review their current consent settings and make changes at any time through their account dashboard. Additionally, the travel agency includes clear explanations of how data will be used and the benefits of opting in, ensuring that users can make informed choices about their data preferences. This approach helps the agency comply with data protection regulations and enhances customer trust by providing transparent and manageable consent options.

Ensuring Accountability:
Accountability under GDPR requires organizations to demonstrate their compliance with data protection principles. This involves maintaining comprehensive records and conducting regular audits.

Maintaining Inventory / Record of Processing (ROP):
Organizations must keep detailed records of their data processing activities, including the types of data processed, the purposes for processing, and any third parties with whom the data is shared etc.[61]

Example:

A global logistics company is overhauling its data management practices as part of a new compliance initiative. The company processes large volumes of sensitive information, including shipment details, customer addresses, and payment information. The current system lacks a comprehensive record of processing activities, leading to difficulties in tracking data usage and ensuring compliance with data protection regulations.

To address the issue, the logistics company implemented a comprehensive Record of Processing (ROP) system that meticulously tracks all data processing activities. This system documents the types of data processed, such as shipment details, customer addresses, and payment information, providing a clear overview of data usage. It includes detailed descriptions of the purposes for which each type of data is processed, such as logistics management and customer service. Access controls are clearly recorded, specifying who has access to different types of data, including internal staff and third-party partners, along with their roles and access levels.

The system also outlined data retention policies, specifying how long various types of data are kept and the criteria for data deletion or anonymization. Additionally, the ROP system includes records of all third parties with whom data is shared, detailing their roles, the nature of the data shared, and the agreements in place to ensure data protection.

This comprehensive approach enhances transparency and compliance with data protection regulations, ensuring responsible data management across the organization.

Conducting Audits:
Regular audits of data processing practices are essential to ensure ongoing compliance with GDPR. These audits should assess whether the organization's practices align with data protection requirements and identify areas for improvement.

Example:

A multinational manufacturing corporation is managing a vast amount of personal data across its global operations, including employee information, customer data, and supplier details. Despite implementing data protection measures, the company recognizes the need to ensure ongoing compliance with GDPR due to the complexity of its operations and the diverse regulatory environments in which it operates.

To maintain compliance with GDPR, the corporation established a rigorous audit process. The company schedules annual audits of its data processing practice across all its global offices. These audits are designed to evaluate whether data processing activities align with GDPR requirements

[61] See *supra* note 12, at 50-51

and identify any compliance gaps. Each office undergoes a detailed review of its data handling procedures, including data collection, processing, storage, and sharing practices. The audit assesses adherence to GDPR principles such as data minimization, purpose limitation, and data subject rights. Findings from these audits are used to address identified gaps and implement corrective measures, ensuring that data protection practices are continuously improved and consistently applied across all locations.

This systematic approach helps the corporation uphold GDPR compliance and strengthen its data protection framework globally.

International Data Transfer Mechanism:
Transfers of personal data from the European Economic Area ("EEA") to countries that have been whitelisted through an adequacy decision by the European Commission[62] are exempt from additional safeguard requirements under the GDPR.To transfer personal data from the EEA or the UK to a non-whitelisted jurisdiction, the controller must:

- implement an appropriate transfer mechanism, such as standard contractual clauses adopted by the European Commission or the UK equivalent;
- conduct a transfer impact assessment ("TIA"); and
- based on the TIA results, implement supplementary measures, such as data encryption in transit and at rest.

Example:

A multinational company headquartered in Germany, an EEA member, plans to transfer the personal data of its European customers to a subsidiary located in Brazil. Since Brazil is not covered by an adequacy decision from the European Commission, the company needs to ensure that the transfer complies with GDPR requirements.

To comply with GDPR for this data transfer, the company taken several key steps.

First, it incorporated Standard Contractual Clauses ("SCCs") adopted by the European Commission into its contract with the Brazilian subsidiary. These SCCs ensure that the data transfer aligns with GDPR standards by providing legal and procedural safeguards. Second, the company conducted a Transfer Impact Assessment (TIA) to evaluate how Brazilian data protection laws compare to GDPR requirements. The TIA involves a thorough analysis of the local legal environment and potential risks to data subjects' privacy. Based on the results of the TIA, the company identifies the need for additional safeguards.
As a result, it implemented encryption measures for data both in transit and at rest, ensuring that the personal data being transferred is protected against unauthorized access and breaches.

This comprehensive approach ensures that the company adheres to GDPR standards and effectively safeguards European customers' personal data during the transfer.

Impact on Consumers:-
GDPR has significantly transformed the relationship between consumers and organizations by integrating DPbDDprinciples. This has led to enhanced consumer privacy rights and greater control over personal data. Below is an elaborated and structured analysis of the GDPR's impact on consumers, illustrated with practical examples:

Enhanced Control Over Personal Data:
GDPR empowers consumers by granting them robust rights to manage their personal data. These rights include:
Right to Access: Consumers can request access to the personal data held by an organization.

[62]Adequacy decisions, European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,commercial%20organisations%20participating%20in%20the (last visited Sept. 7, 2024).

Example:A customer of an online retail store can ask for a copy of all the personal information the store has collected about them, such as purchase history, contact details, and preferences.

Right to Rectification: If a consumer notices that their data is incorrect or outdated, they have the right to request corrections.

Example: An insurance company has an incorrect address on file, the consumer can request that this information be updated.

Right to Erasure (Right to be Forgotten): Consumers can request the deletion of their personal data under certain conditions.

Example:A user closes their account with a social media platform, they can ask the platform to delete all associated personal data.
These rights give consumers unprecedented control over their personal information, ensuring it is accurate, relevant, and used according to their preferences.

Increased Transparency in Data Practices:-
Clear and Accessible Information: GDPR mandates that organizations provide transparent and easily understandable privacy notices, making it clear how consumer data is collected, processed, and shared.

Example:A mobile app that collects location data must clearly inform users through a privacy notice about how their location information will be used, whether it will be shared with third parties, and for how long it will be stored. This transparency allows consumers to make informed decisions, such as opting out of location tracking if they feel it infringes on their privacy.

Improved Security of Personal Data:-
Mandatory Security Measures: GDPR requires organizations to implement stringent security measures to protect personal data from unauthorized access, breaches, and cyberattacks.

Example:A financial services company that processes credit card information must implement encryption and multi-factor authentication to protect this sensitive data.

As a result, consumers benefit from a reduced risk of identity theft and unauthorized use of their financial information, providing them with greater peace of mind.

Stronger Accountability and Trust:-
Demonstrating Compliance: Under GDPR, organizations must demonstrate their compliance with data protection principles through documentation, regular audits, and adherence to best practices. This fosters a culture of accountability.

Example: An e-commerce platform must maintain detailed records of its data processing activities and conduct regular audits to ensure compliance with GDPR. If a consumer files a complaint about their data being mishandled, the organization is required to provide evidence of its compliance efforts, thereby enhancing consumer trust in the platform's commitment to data protection.

In conclusion, the GDPR framework not only mandates compliance with data protection regulations but also emphasizes the strategic value of proactive privacy management. DPbDDprinciples serve as a foundation for embedding privacy considerations into the very fabric of organizational processes, from the initial stages of project development to the ongoing management of personal data. This proactive approach not only ensures that businesses adhere to legal requirements but also strengthens their resilience against data breaches and enhances their reputation in a competitive marketplace.By integrating privacy into their core practices, organizations can build stronger, trust-based relationships with consumers and stakeholders. Consumers are increasingly aware of their rights under GDPR, and their expectations for transparency, security, and control over personal data have never been higher. Businesses that prioritize these aspects demonstrate their commitment to respecting individual privacy, which can lead to increased customer loyalty, a more positive brand image, and a competitive advantage.Moreover, in an era where

data breaches and privacy violations can result in significant financial and reputational damage, adopting DPbDDand other GDPR-compliant practices is not just a regulatory obligation but a strategic imperative. Companies that take privacy seriously are better positioned to navigate the complexities of the digital age, protect their assets, and sustain their growth. Ultimately, by embedding privacy into their business model and honoring consumer rights, organizations can drive long-term success while contributing to a more secure and trustworthy digital ecosystem.

India's Digital Personal Data Protection Act:-

DPDPA, enacted in 2023, represents a crucial evolution in the country's data protection landscape. It aims to modernize India's approach to personal data protection by aligning with global standards while addressing the unique needs of the Indian digital economy. The Act provides a comprehensive framework to safeguard personal data, empowering individuals with rights over their data and imposing stringent obligations on organizations.

Objectives: The DPDPA addresses several core objectives:

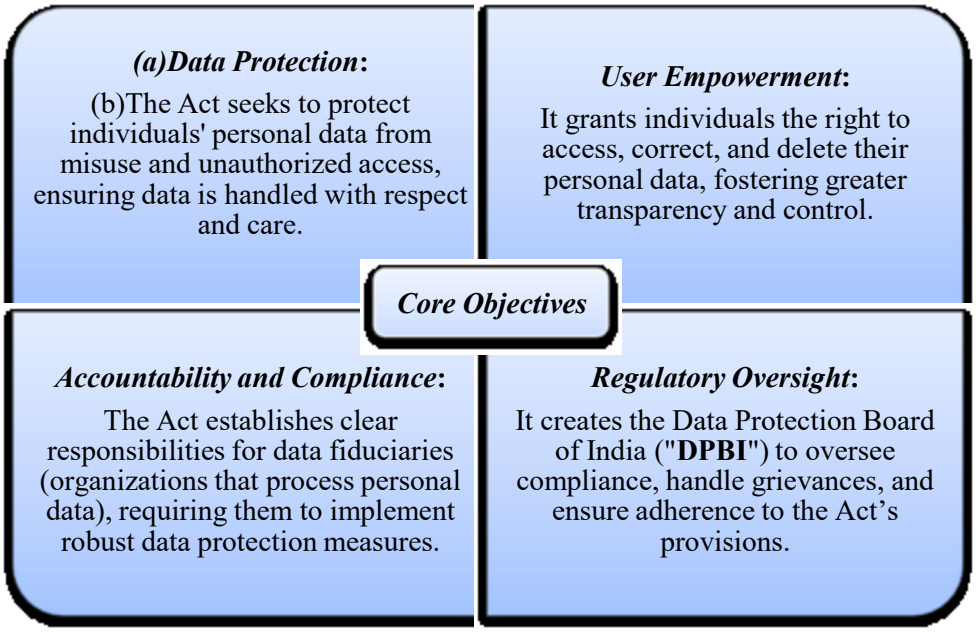

Figure 7 – DPDPA Core Objectives

Key Provisions:

(a)Data protection principles: While the Act does not explicitly mention data protection principles, the Citizens' Data Security and Privacy Report submitted to the Lok Sabha (the Lower House of the Indian Parliament) on August 1, 2023, provides insight into the Act's legislative background and key considerations. This report highlights the Act's alignment with internationally recognized data protection standards.[63]Chapter 2 of the DPDPA[64] outlines the responsibilities of data fiduciaries and the conditions under which they are authorized to process personal data. It establishes essential principles for managing personal data, aligning with international data protection standards.

[63]Standing Committee on Communications and Information Technology, Ministry of Electronics and Information Technology, Citizens' Data Security and Privacy (2023), https://eparlib.nic.in/bitstream/123456789/2505169/1/17_Communications_and_Information_Technology_48.pdf#search=null%2017%20Departmentally%20Related%20Standing%20Committees

[64] Digital Personal Data Protection Act, No. 22 of 2023, § Ch. II (Ind.)

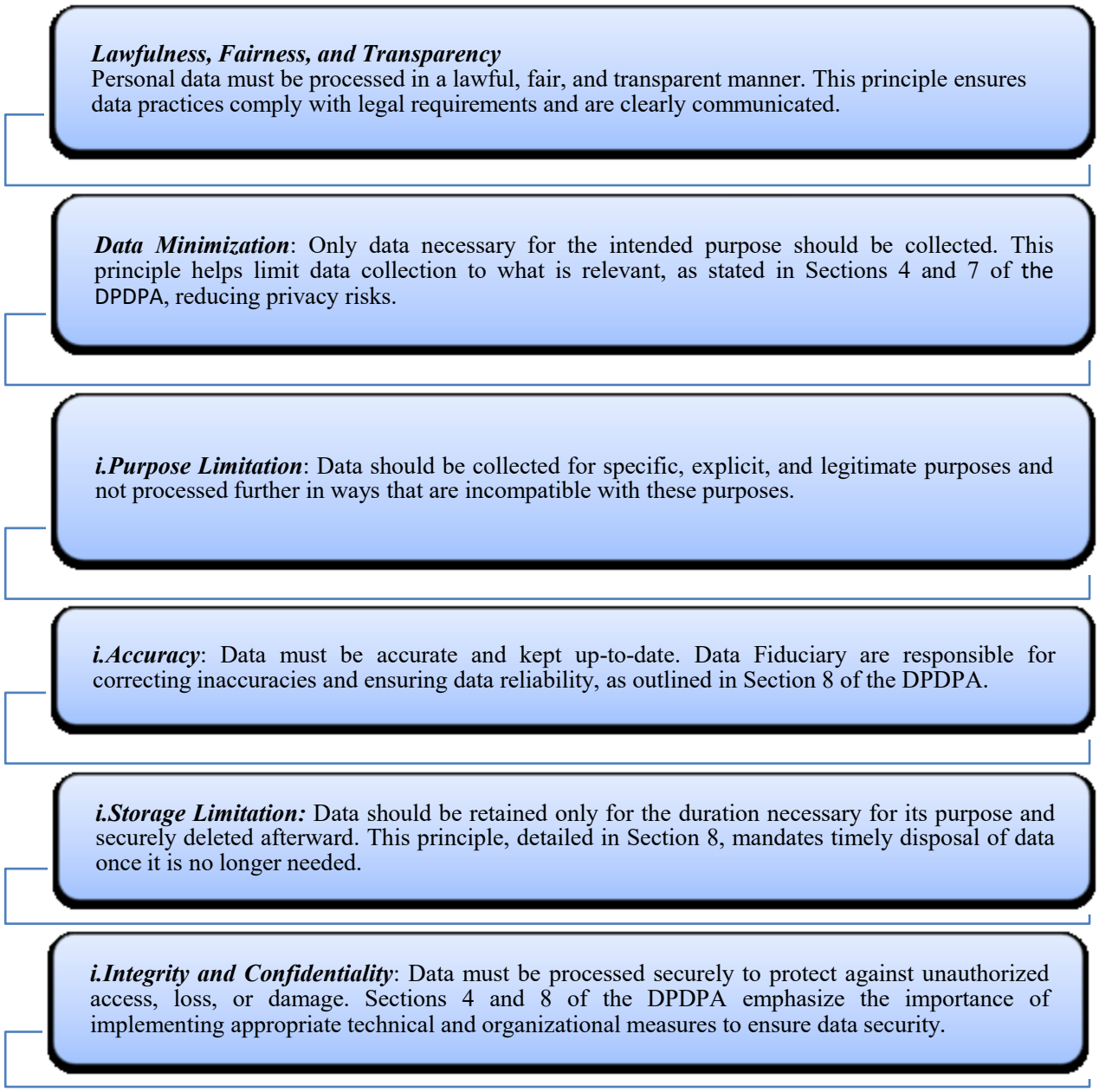

Figure 8 – DPDPA Data protection principles

(b) Lawfulness of processing:
The DPDPA mandates that data fiduciaries must have a lawful purpose for all processing activities. However, unlike the GDPR, which offers a list of lawful grounds, the DPDPA primarily requires data fiduciaries to obtain consent for processing personal data. In certain situations, they may rely on "legitimate use" conditions.[65]

(c)Consent& Notice:
Consent is central to the DPDPA. Section 6 of the DPDPA[66]introduces new consent protocols, marking a significant shift from the current standards for data fiduciaries. Under the existing Information Technology (Reasonable

[65] Digital Personal Data Protection Act, No. 22 of 2023, § 7 (Ind.)
[66]Id., § 6 (Ind.)

security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules"), organizations are required to obtain written consent when collecting "sensitive personal data," which encompasses a detailed and exhaustive list of data categories.[67] Although the DPDPA does not distinguish between personal data and sensitive personal data, it broadens the requirement to cover all personal data. The Act enforces a stricter standard for consent by mandating a 'clear affirmative action'[68].

Under the DPDPA, consent is the foundation of personal data processing and must meet stringent criteria to be valid. Consent must be free, specific, informed, unconditional, and unambiguous. This means that the data principal's agreement must be provided through a clear affirmative action, such as checking a box or clicking "I agree," indicating their willingness to allow their personal data to be processed for a specified purpose. Pre-ticked boxes or implied consent are not sufficient.In addition to consent, Section 7 recognises "legitimate uses" – including voluntary disclosure by the data principal, performance of legal functions, emergencies and compliance with judicial or regulatory orders. These bases permit certain processing without consent when reasonably expected or mandated by law, underscoring that the DPDPA is not purely consent-centric.

Additionally, the data principal has the right to withdraw their consent at any time, with the same level of ease as when it was initially given.[69] Upon withdrawal, any further processing must cease, and the data must be erased, unless required otherwise by law.[70]Every request for consent must be accompanied by a notice that clearly informs the data principal about the personal data being collected, the purpose of processing, and the methods available for withdrawing consent and lodging complaints with the DPBI.[71] This notice should be available in English and in any of the languages specified in the Eighth Schedule of the Indian Constitution[72], ensuring that the data principal can understand the information in their preferred language.

Finally, while consent is the primary basis for processing, the DPDPA also allows for certain 'legitimate uses' where processing may occur without explicit consent. These exceptions include scenarios such as:[73]
(i) Voluntary disclosure by data principal.
(ii) Reasonable expectation by data principal.
(iii) Performance of function under the law.
(iv) Medical emergency among others.
(v) Compliance with any judgment issued under any law.
(vi) Threat to public health.
(vii) Ensure safety in case of any disaster.

(d) Consent Manager: The DPDPA designates the "Consent Manager" as a central authority, a key element of the consent management architecture recommended by the Justice B.N. Srikrishna Committee[74]. Individuals will be able to give, manage, review, or withdraw consent through a "consent manager" under the DPDPA. A consent manager, registered with the DPBI, will act as a central point of contact, offering various consent options to data principals via a transparent, accessible, and interoperable platform.[75]The consent manager must (i) be accountable to the data principal and (ii) act on their behalf, in accordance with prescribed obligations.[76]

[67] The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Gazette of India, Rule 3 (Apr. 11, 2011),https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf
[68]Id., § 6(1) (Ind.)
[69]Id., § 6(4) (Ind.)
[70]Id., § 8(7) (Ind.)
[71]Id., § 5(1) (Ind.)
[72]Id., § 5(3) (Ind.)
[73] See supra note 65.
[74] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Report,27(2018),https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf
[75]Id., § 2(g) (Ind.)
[76]Id., § 6(8) (Ind.)

(e) Data principal rights:Data principals, also known as data subjects or users, are individuals whose personal information is collected and processed by an organization referred to as the data fiduciary. The DPDPA outlines specific rights for data principals but also imposes certain obligations on them when exercising these rights. Individuals must refrain from impersonating others[77], registering false or frivolous grievances[78], or providing false identity information[79]. Additionally, while the rights of data subjects apply to data fiduciaries, they do not extend directly to data processors—though such obligations may be enforced through contractual agreements.The DPDPA establishes the following rights for data principals:

Right of Access: Upon the data principal's request, a data fiduciary is required to provide the following information:[80]

- a summary of the personal data being processed by the data fiduciary and the activities they are performing with that data;
- the identities of any other data fiduciaries and data processors with whom the data fiduciary has shared the personal data, along with a description of what was shared; and
- Any other information related to the personal data and its processing, as required.

Right to Rectification: Upon receiving a request from the data principal to correct, complete, or update their personal data, the data fiduciary shall:[81]

- Correct any inaccurate or misleading personal data;
- Complete any incomplete personal data; and
- Update the personal data as requested.

Right to Erasure: Upon receiving an erasure request, the data fiduciary shall delete the personal data unless its retention is necessary for a specified purpose or required by any applicable law.[82] However, it is unclear whether this right to erasure includes the right to be forgotten, as it appears to be explicitly dependent on the expiration of the processing purpose.

Right of grievance redressal:[83]A data principal shall have the right to access readily available grievance redressal mechanisms provided by a data fiduciary or consent manager for any act or omission related to their obligations concerning the data principal's personal data or the exercise of the data principal's rights under this Act and its rules. The data fiduciary or consent manager must respond to such grievances within the prescribed period from the date of receipt, as applicable to all or specific classes of data fiduciaries. The data principal must exhaust this grievance redressal process before approaching the DPBI.

Right to nominate: A data principal has the right to designate another individual, in a prescribed manner, who will assume and exercise the rights of the data principal in the event of their death or incapacity.[84]In conclusion, while the GDPR provides a more comprehensive set of rights for data subjects, the DPDPA takes a more limited approach. Under the GDPR, data subjects have the explicit right to object to or restrict the processing of their personal data, allowing them greater control over how their data is used. In contrast, the DPDPA does not provide specific instances where data principals can object to or restrict data processing. Instead, it grants them the right to withdraw consent, which obliges data fiduciaries and processors to cease processing the relevant personal data.Moreover, the DPDPA does not include provisions for the right to data portability, meaning it does not address the ability of data principals to transfer their data from one data fiduciary to another. This contrasts with the GDPR, which explicitly provides this right, facilitating greater data mobility and user control.Lastly, the DPDPA does not contain specific provisions regarding the right not to be subject to automated decision-making, particularly those with legal or similarly significant effects. The GDPR, on the other hand, addresses this concern by granting data subjects

[77]Id., § 15(b) (Ind.)
[78]Id., § 15(d) (Ind.)
[79]Id., § 15(c) (Ind.)
[80]Id., § 11(1) (Ind.)
[81]Id., § 12(2) (Ind.)
[82]Id., § 12(3) (Ind.)
[83]Id., § 13 (Ind.)
[84]Id., § 14 (Ind.)

protection against decisions made solely through automated processing, ensuring that individuals have recourse in such situations.Overall, while the DPDPA introduces important data protection rights, it does not encompass the full range of protections offered by the GDPR, particularly concerning objection to processing, data portability, and safeguards against automated decision-making.

Integration of Privacy by Designin DPDPA:-
DPDPA does not explicitly mention the PbD principle. However, it imposes obligations on data fiduciaries to implement appropriate 'technical and organizational measures' to ensure compliance with the Act.[85] These obligations include establishing security safeguards to prevent personal data breaches. While the Act does not directly reference PbD, the required implementation of these measures inherently involves incorporating several well-recognized PbDpractices.

Practical Implications for Organizations:-
Impact on Businesses:-
The DPDPA significantly impacts businesses by requiring them to implement appropriate 'technical and organizational measures' to safeguard personal data. As businesses work to comply with the DPDPA, they naturally incorporate practices such as minimizing data collection, ensuring data accuracy, and embedding privacy controls etc. within their systems and processes. This de facto adoption of PbD practices, driven by the need for robust data protection, positions businesses to enhance their privacy standards, ultimately building consumer trust and improving compliance with global data protection frameworks.

Conducting Data Protection Impact Assessments (DPIAs): DPIAs are crucial for evaluating privacy risks in data processing activities. 'Significant Data Fiduciary' is required to conduct periodic DPIAs to evaluate and manage privacy risks associated with their data processing activities.[86] These assessments help identify, assess, and mitigate privacy risks, ensuring compliance with the DPDPA. The DPIA process involves detailing the rights of data principals, the purpose of processing their personal data, and addressing other prescribed matters related to privacy risk management.

Example:

A leading financial technology firm has recently introduced an AI-based app designed to deliver personalized investment strategies and comprehensive financial planning advice. This app utilizes sophisticated algorithms to analyze users' financial data, including detailed income streams, historical investment performance, spending patterns, credit scores, and future financial goals.
Data Protection Impact Assessment (DPIA) (Given the sensitive nature of the data and the reliance on advanced AI technologies, a robust DPIA is essential.)
1. **Risk Assessment Implementation**: The DPIA evaluated risks associated with the app's handling of personal financial data and its AI-driven recommendations, involving a detailed review of data collection, processing, storage, and third-party integrations. 2. **Risk Identification:** (a) Data Sensitivity and Volume: The app handles extensive sensitive financial data, posing risks of breaches, unauthorized access, and misuse. (b) AI Model Accuracy and Bias: Risks include inaccuracies and biases in AI algorithms, which could lead to incorrect financial advice and discriminatory outcomes. (c) Data Retention and Minimization: Ensuring that personal financial data is retained only for as long as necessary for the app's purposes and implementing data minimization practices to avoid excessive data collection. The risk involves managing the lifecycle of data and ensuring it is not kept beyond its useful period. (d) Third-Party Processing: The app integrates with various third parties for data storage, analytics, and enhanced financial services. Risks include data leakage or non-compliance by

[85]Id., § 8(4) (Ind.)
[86]Id., § 10(2)(c)(i) (Ind.)

third-party partners.

3. **Risk Assessment and Mitigation:**
(a) Enhanced Security: Implementing end-to-end encryption, advanced access control mechanisms, and multi-factor authentication to protect sensitive financial data. Regular penetration testing and vulnerability assessments are conducted to identify and address security weaknesses.
(b) AI Validation and Transparency: Regularly validating and auditing AI algorithms to ensure their accuracy and fairness. Providing transparency to users about how AI models are trained, the data they use, and how recommendations are generated. Implementing mechanisms to address and rectify algorithmic biases.
(c) User Consent and Access: Implementing a robust consent management system and providing users with control over their data.

By performing an in-depth DPIA, the financial advisory app effectively manages complex privacy risks associated with advanced AI technology and sensitive financial data. The app demonstrates a strong commitment to data protection, builds user trust through transparent practices, and ensures robust compliance with the DPDPA**.**

Implementing Data Minimization: The DPDPA emphasizes the principle of data minimization, encouraging organizations to collect only the data necessary for the specified purpose. This principle applies particularly when consent is the legitimate basis for data collection.Implementing data minimization in a business context requires careful planning, as the benefits for businesses are substantial:

a) **Reduced Risk:** By limiting data collection, businesses inherently lower the risk of data breaches, unauthorized access, and potential financial and reputational damage.
b) **Enhanced Privacy:** Retaining only essential data minimizes the potential for privacy violations and misuse, which is increasingly important in building and maintaining customer trust.
c) **Regulatory Compliance:** Adhering to data minimization principles ensures alignment with regulatory requirements, reducing the likelihood of legal issues and penalties.

Examples:

A leading health application designed sophisticated tracking tools and personalized health management features. The app collects extensive user data, including daily dietary intake, exercise routines, and detailed sleep patterns, to deliver tailored health recommendations and facilitate comprehensive wellness tracking.

The app now limits data collection to essential metrics like step count and basic exercise duration. Detailed logs are only collected when users actively seek advanced features, such as customized diet plans, and are otherwise kept minimal to enhance privacy.

A financial institution employed advanced analytics platforms and machine learning algorithms to enhance its fraud detection capabilities. The institution processes a broad spectrum of customer transaction data, including spending habits and transaction details, to refine its fraud detection systems and offer personalized financial advice.

The institution revised its processing protocols to focus solely on transaction patterns relevant to fraud detection. Personal data not directly related to fraud prevention, such as demographic information, is processed only when needed for specific analyses and then promptly discarded.

A major e-commerce platform utilizes extensive customer purchase history and browsing behavior data to drive its recommendation algorithms and marketing strategies. The platform retains detailed records of user interactions, including past purchases and product views, to optimize user experience and targeted promotions.

The platform implemented a retention policy where purchase history is stored only for a set period (e.g., 12 months) and is anonymized after this period. Browsing data is kept only as long as needed to refine search algorithms, with user consent obtained for any extended retention.

A leading smart home device manufacturer develops advanced automation systems and monitoring tools. These devices gather detailed usage data, such as temperature settings, energy consumption, and user preferences, to enhance home automation features and provide insightful usage reports.
The device now processes and stores data locally on the device itself, with only aggregated usage patterns sent to the cloud. Detailed, personal data is accessed only when necessary for troubleshooting or specific user-requested features, adhering to strict data retention and anonymization practices.

Enhancing Transparency: Transparency is a fundamental requirement under the DPDPA, requiring organizations to clearly communicate their data processing practices to users, ensuring they understand how their personal data is being utilized. The DPDPA extends beyond mere compliance with data processing protocols, emphasizing the importance of data ethics. This involves adhering to principles that ensure data collection and processing are fair, transparent, non-arbitrary, and non-discriminatory, all conducted in line with ethical standards.

Updating Privacy Notices: The DPDPA mandates that organizations provide a notice to data principals either at or before obtaining their personal data. This notice must include: (i) the specific personal data being collected and the purpose for its processing; (ii) the means by which data principals can exercise their rights under the DPDPA concerning their personal data; and (iii) the process for lodging a complaint with the DPBI.[87]

Example:

A telecommunications company is launching a new mobile service that involves collecting customer data like location, call records, and browsing history. However, the company's existing privacy notices are outdated, difficult to understand, and not easily accessible, risking non-compliance with the DPDPA.
The company revamps its privacy notices to align with DPDPA requirements. The updated notices clearly explain what data is collected, why it's processed, and how customers can exercise their rights under the DPDPA. These notices are made easily accessible on the company's website and mobile app. This ensures compliance and builds customer trust through enhanced transparency.

Implementing Consent Mechanisms: Under the DPDPA, implementing effective consent mechanisms is crucial for lawful data processing. Organizations must obtain informed, explicit, and freely given consent from individuals before collecting or processing their personal data, with the option for consent to be withdrawn at any time. Detailed records of consent, including identifiers, timestamps, and the version of the consent notice etc., must be maintained to demonstrate compliance with the law. The DPDPA also introduces the concept of Consent Manager—registered entity that manages consent on behalf of data principal(s).[88] Additionally, consent requests must be communicated in clear and simple language, with the option to access the request in English or any language specified in the Eighth Schedule of the Constitution of India.[89]This ensures transparency and accessibility, allowing all users to understand and control their data processing choices. These mechanisms are vital for establishing a lawful basis for data processing, ensuring compliance with the DPDPA, and upholding individuals' data autonomy and protection.

[87] See supra note 71.
[88] See supra note 75.
[89] See supra note 72.

Examples:

A healthcare provider, "MediCHealth," is rolling out a new electronic health record (EHR) system designed to enhance patient care and streamline data management. The existing consent forms used by the company are general and do not specify the particular purposes for which patient data is used. This setup does not meet the regulatory requirements for explicit consent. Additionally, the system lacks features for patients to provide itemized consent or to manage their consent preferences easily.
Medi C Health updated its consent process to comply with data protection regulations. The revised consent forms now clearly outline the specific types of data collected, such as medical history and test results, and detail the exact purposes for processing this data, including treatment planning, billing, and research. Patients are also informed about how they can exercise their rights or file complaints with the Data Protection Board. Furthermore, the company conducted a thorough audit of existing data to ensure that previous consents meet the new standards. The EHR system is upgraded to enable patients to provide itemized consent for different purposes and to modify their consent preferences at any time. These changes ensure that patient consent is free, specific, informed, and unambiguous, thereby aligning with legal requirements. .

A health insurance provider in India, aiming to comply with the DPDPA, needs to ensure that its privacy notices are available in multiple languages. This task is complex due to the need for accurate translations and ensuring accessibility for all users.
The provider implemented a robust system for managing privacy notices across multiple languages. They partnered with a certified translation agency to translate the privacy notices into the 22 required languages. The translated notices are then integrated into their digital platforms, including their website and mobile app, where users can easily select their preferred language. The provider also established a process for regular review and updates to ensure that the translations remain accurate and the notices comply with evolving regulations. This approach effectively meets the requirements of the DPDPA and enhances user transparency and accessibility.

A telecommunications company in India appointed a Consent Manager to comply with the DPDPA. This registered Consent Manager enables users to easily give, manage, review, or withdraw their consent for data processing through a clear and accessible platform integrated into the company’s website and app.
The telecommunications company integrated the Consent Manager into its system, allowing users to interact with it through a user-friendly interface on the company's website and mobile app. The platform is designed to be clear and intuitive, providing users with straightforward options to adjust their consent settings. The Consent Manager maintains records of all consent transactions and ensures that these records are kept up-to-date, aligning with the requirements of the DPDPA.

A global financial services firm operating in India aims to comply with the stringent requirements of the DPDPA, which requires explicit 'opt-in' consent from clients for each data processing activity. Unlike an 'opt-out' approach, where clients can withdraw consent after being informed, the firm has implemented a system to obtain clear affirmative consent through detailed forms, eliminating pre-checked boxes and any form of implied consent.
The firm implemented a state-of-the-art consent management system designed to ensure rigorous compliance with data protection regulations. This system features interactive consent forms that require clients to actively opt in for each specific data processing activity, eliminating pre-checked boxes and guaranteeing explicit consent.A centralized, real-time consent management

dashboard has been developed, allowing clients to seamlessly review, update, and manage their consent preferences across digital platforms. Automated consent tracking ensures accurate documentation of every consent action, while an automated notification system promptly alerts clients to any changes in data processing practices that necessitate new or updated consent.Additionally, advanced analytics tools are utilized to monitor compliance, track consent patterns, and generate actionable insights for ongoing enhancement of consent management processes.

A global educational services company operates online learning platforms, including interactive educational apps and virtual classrooms, catering to a diverse audience, including children under 18. To comply with the DPDPA, which mandates obtaining verifiable parental or guardian consent for processing data of children, the company faces logistical challenges. These include ensuring that consent is genuinely obtained and not merely implied, given the high threshold for consent defined under the DPDPA. Additionally, the company needs to manage and verify consent for different data processing activities across its various platforms, which may lead to operational complexities and potential risks of non-compliance.

The company developed an integrated parental consent management system within its online learning platforms. This system employs multi-factor authentication to ensure that parental consent is genuinely obtained rather than implied. It includes age verification mechanisms that direct users under 18 to the appropriate parental consent process, thus preventing unauthorized access. Additionally, the system features a centralized, secure repository for tracking and managing consent records.The company has also incorporated clear and accessible communication channels within the system to keep parents informed about data processing activities and their rights. Regular updates are provided via email, in-app notifications, and dedicated helpdesk support to ensure that information is presented clearly and understandably. User-friendly consent interfaces are designed within educational apps and virtual classrooms, allowing parents to review data processing activities and provide consent through explicit affirmative actions. Automated compliance monitoring tools are used to track consent status and generate real-time reports, helping the company maintain compliance and promptly address any potential issues.

Stream8, a popular online media streaming platform, relies heavily on cookies to enhance user experiences by remembering viewing history, suggesting personalized content, and tracking engagement metrics. To meet stringent privacy regulations and ensure user trust, Stream8 is in the process of addressing cookie consent management comprehensively.

Stream8 integrated a prominent cookie consent banner that activates upon users' first visit to the site. This banner informs users that Stream8 uses cookies to personalize their viewing experience and analyze content engagement. It clearly specifies that cookies will only be set after users actively provide their consent. The banner ensures all consent checkboxes are unmarked by default, allowing users to make an informed choice. The platform classifies cookies into two categories: strictly necessary cookies essential for streaming and user authentication, and non-essential cookies used for analytics and marketing. Users can opt to enable only the strictly necessary cookies if they prefer not to share additional data.

Stream8 further included a comprehensive cookie notice linked from the consent banner. This notice details the types of cookies used, their purposes, and the duration they remain active. Additionally, it links to a full cookie policy that explains how cookies are utilized and any third-party partnerships involved. An accessible opt-out mechanism is also available in the user account settings, allowing users to modify or withdraw their cookie preferences at any time.

Ensuring Accountability: The DPDPA's core principles emphasize accountability, holding entities responsible for data breaches and violations. Effective data governance is essential for privacy compliance. While the Act doesn't

mandate a data inventory or map, privacy professionals must understand the personal data being processed—its types, storage locations, processing activities, and involved data processors. This understanding is key to fulfilling the Act's obligations, including ensuring data accuracy and consistency, enabling data principals to exercise their rights (such as access, correction, and erasure), enforcing data erasure when necessary, and providing clear notice about data processing.

Data Mapping and Maintaining Inventory: Choosing the right approach for data inventory and mapping requires privacy professionals to actively evaluate various methods, ranging from manual techniques like interviews and questionnaires to automated tools such as code scanning and machine learning-based classification. When deciding on the best method, they should consider factors like the complexity of the data ecosystem, data volume, resource needs, executive support, tool availability, and scalability.

Example:

FinTech Global, a fast-growing financial technology company, is expanding into multiple international markets, each with unique regulatory demands. The company handles large volumes of sensitive personal data across various platforms, including cloud services and third-party vendors. With inconsistent data governance practices across regions and a need for efficient compliance with the DPDPA, FinTech Global faces the challenge of implementing a unified, scalable data mapping and inventory solution.
FinTech Global adopted a hybrid data mapping approach. The company begins with manual interviews and questionnaires to capture critical data processes across regions, followed by deploying automated tools like code scanning and machine learning for handling large data volumes and providing a comprehensive view of operations. After a successful pilot in Europe, this tailored strategy is rolled out globally, ensuring efficient compliance with regional regulations and scalability as the company continues to grow. Continuous monitoring and regular updates to the data inventory further ensure that FinTech Global stays ahead of regulatory changes, maintaining robust data governance and operational efficiency.

(b) Data retention: Upon receiving a request from a data principal, the data fiduciary must erase the personal data unless its retention is necessary for the specified purpose or required by law. Furthermore, the data fiduciary must erase the personal data when the data principal withdraws consent or when it is reasonable to assume that the specified purpose is no longer being served, whichever occurs first.[90] The data fiduciary is also responsible for ensuring that any data processor to whom the data was provided for processing also erases the personal data.[91]The specified purpose shall be considered no longer served if the data principal neither approaches the data fiduciary for the performance of the specified purpose[92] nor exercises any of their rights related to the processing for a prescribed period. This period may vary depending on the class of data fiduciaries and the purpose of the data processing.[93]

Examples:

Emma, an individual, registers on SellIt, an online marketplace run by TechTrade, to sell her vintage furniture. After consenting to TechTrade processing her personal data to facilitate the sale, she successfully completes the sale and closes her listing. Emma then requests that TechTrade erase her personal data from their system.
TechTrade reviewed Emma's request and confirmed that the purpose for which her data was collected (i.e., selling the furniture) had been fulfilled. Since there was no ongoing need to retain Emma's personal data and no legal obligation to keep it, TechTrade promptly deleted her personal data from its systems. Additionally, TechTrade ensured that any third-party data processors who had access to Emma's data also erased it. This action complied with the requirement to erase personal data when it was no longer necessary for the specified purpose.

[90]Id., § 8(7)(a) (Ind.)
[91]Id., § 8(7)(b) (Ind.)
[92]Id., § 8(8)(a) (Ind.)
[93]Id., § 8(8)(b) (Ind.)

John, a client of SecureBank, decides to close his savings account. SecureBank is subject to financial regulations that require it to retain records of client identities for ten years after account closure for compliance and audit purposes. John requests that his personal data be deleted upon closing his account.
SecureBank informed John that, despite his request for data erasure, the bank must retain his personal data for ten years due to legal requirements. SecureBank ensures that John's data is securely stored and protected during this period. Once the ten-year retention period expires, SecureBank will proceed with the permanent erasure of John's personal data. In the meantime, the bank maintains transparency with John about the retention period and the data protection measures in place. This approach aligns with the legal obligation to retain data while ensuring compliance with data protection standards

RetailCo, a large retail company, collects various types of personal data from its customers, including purchase history, loyalty program information, and marketing preferences. Currently, RetailCo retains this data indefinitely to maintain customer profiles and optimize marketing strategies. The company's privacy policy mentions broad retention periods but lacks specifics and does not include periodic reviews or anonymization practices.
RetailCo started by categorizing its data into groups such as purchase records, loyalty program data, and marketing preferences. It then reviews relevant data protection laws to determine the appropriate retention periods for each category—e.g., retaining purchase records for up to five years for tax compliance and reviewing marketing data annually.RetailCo assessed its business needs and identified outdated marketing data as no longer useful. Subsequently, it developed specific retention policy, such as deleting purchase records older than five years and anonymizing marketing data after two years of inactivity. The company communicated the updated policy to employees and customers, and established a system for documenting retention periods and data categories.

(c) Implementing data Breach notification mechanism:Organizations must actively protect personal data by implementing effective security measures to prevent breaches. The DPDPA requires these safeguards to prevent and manage data breaches, ensure proper data processing, and uphold data protection principles. A strong breach management process, including clear investigation protocols and robust internal and external reporting mechanisms, is essential for mitigating financial, reputational, and legal risks. This enables organizations to respond swiftly and effectively to data breaches in today's digital environment.

Example:

TechCo, a technology firm, discovers a breach where unauthorized access to customer data has occurred. The breach includes not just data loss but also unauthorized alterations and potential misuse.
TechCo faces a data breach involving sensitive customer information and implements a robust response strategy. They defined personal data breaches broadly, beyond mere data loss, and utilize AI-powered monitoring tools to detect anomalies and unauthorized access in real-time. Advanced forensic AI tools then assess the breach's scope, compromised data, and risks. For timely notifications, TechCo employed automated systems to alert affected individuals and regulatory bodies, crafting communication plans adjusted in real-time with AI assistance. Post-breach, they use AI for root cause analysis, addressing vulnerabilities, and enhancing security measures.

(d) Ensuring accountability and security in Third-party data sharing: Organizations must be transparent, accountable, and vigilant in their third-party data-sharing activities to ensure lawful and secure handling of personal

data. They should oversee third-party ('data processors') personal data processing to guarantee that it is done securely and for the intended purposes. A data fiduciary may only engage, appoint, or involve a data processor to manage personal data on its behalf for providing goods or services to data principals if a valid contract is in place.[94]Despite data processors being bound by agreements with data fiduciaries, the DPDPA, places the responsibility for protecting personal data shared with these processors on the data fiduciaries themselves.

Example:

An e-commerce platform, "ShopS," partners with several third-party service providers, including a marketing analytics firm, "MarketAnalyzr," and a payment processing company, "PaySecure." ShopScollects extensive customer data, including purchase histories, browsing habits, and payment details. ShopS shares this data with MarketAnalyzr to tailor marketing strategies and with PaySecure to process transactions. Despite these partnerships, ShopS's data privacy notice on its website only contains generic statements about sharing data with third parties without specifying how MarketAnalyzr or PaySecure use the data.
ShopS updated its contracts with MarketAnalyzr and PaySecure to specify data privacy obligations, including security measures, data use limitations, and compliance with the DPDPA. It conducted a detailed data mapping exercise to track all data flows and ensures processors handle data according to these agreements. To protect personal data, ShopS implemented encryption and secure transfer protocols and mandated regular security assessments from processors. The company also implemented a system to promptly cease data processing and erase personal data upon customer consent withdrawal and schedules periodic audits to verify compliance and address any issues.

International Data Transfer Mechanism: The DPDPA allows the government to impose restrictions on data transfers to specific countries through a designated list.[95] Until such a list is issued, data transfers are broadly permitted to all countries. The DPDPA's framework provides the government with considerable leeway to impose restrictions, but currently, there are no specific notifications or Digital Personal Data Protection Rules available for guidance.Legislative history indicates that future restrictions may align with international standards, similar to the EU's GDPR. Potential measures could include adequacy assessments to ensure that the data protection level in the destination country meets Indian standards. Additional conditions might involve implementing legal, technical, and organizational safeguards, such as standard contractual clauses or binding corporate rules. Explicit user consent for cross-border data transfers could also become a requirement.Presently, no countries are blacklisted, and no restrictions are enforced, but this could change with new DPDP Rules. Additionally, stricter data transfer laws in India's sector-specific regulations will override the DPDPA's general provisions.[96]

Example:

A multinational bank, "AED Ltd.", aims to enhance its global data analytics by integrating cutting-edge AI tools to analyze payment systems data. To achieve this, the bank plans to consolidate its data across international data centers for more efficient global processing.
The Bank must comply with the applicable circular issued by the Reserve Bank of India ("Circular"), which requires that payment systems data be stored within India. This regulatory mandate necessitates that the Bank either set up new local data centers in India or utilize existing ones to ensure compliance, even though it seeks to perform global analytics.Bank adopted a data segmentation strategy to meet the Circular. This strategy keeps payment systems data within its Indian data centers, while other data is processed on its global platforms. By establishing local data facilities and using a hybrid data management approach, the Bank not only complies with Indian regulations but also leverages advanced global analytics tools for broader insights.

Impact on Consumers

[94]Id., § 8(2) (Ind.)
[95]Id., § 16(1) (Ind.)
[96]Id., § 16(2) (Ind.)

For consumers, the DPDPA's approach to data protection, while different from the GDPR, still offers substantial privacy safeguards. By requiring organizations to implement stringent security measures, the Act indirectly fosters a privacy-conscious environment that benefits consumers. This approach enhances consumer confidence by providing them with rights and protections that, while not as comprehensive as those under GDPR, still offer significant control over their personal information. As a result, consumers can expect a level of data protection that, though not as explicitly framed around PbD, effectively achieves many of the same outcomes.

Enhanced Control Over Personal Data: Under DPDPA, consumers are empowered with robust rights to manage their personal data, reflecting a user-centric approach to privacy. These rights include:

(a) Right to Access: Consumers have the right to request access to the personal data an organization holds about them. This ensures transparency and allows consumers to be informed about how their data is being used.

Example:A client of a large financial institution can request a comprehensive report detailing all the personal data the bank has collected, such as account balances, loan details, and communication logs. The report will also identify other organizations, like credit bureaus or financial advisors, with whom this data has been shared, and explain what specific data was shared with each. This right allows the client to fully understand how their financial and personal information is being used and shared, ensuring transparency while also acknowledging that some data shared with government agencies for legal investigations may not be disclosed.

Right to Rectification: Consumers have the right to request corrections, updates, or completion of their personal data if it is incorrect, outdated, or incomplete. A data principal can seek these adjustments for data previously consented to, in accordance with theAct.

Example: A customer named Alex Taylor notices that their mailing address is outdated in their healthcare provider's records, affecting the delivery of critical health communications. Alex logs into their online patient portal and submits a detailed request to update the address. This request includes supporting documentation, such as a recent utility bill and a government-issued ID, to verify the new address. The healthcare provider's system processes the request, which triggers an internal review to ensure all related records, such as insurance information and appointment details, are also updated. The provider then confirms the address change and ensures that all future correspondence, including medical bills, appointment reminders, and health records, are sent to the corrected address, avoiding any disruption in the delivery of essential health information.

.

Right to Erasure: Consumers can request the deletion of their personal data under certain conditions.

Example: A customer named Jamie Lee requests the deletion of their personal data from a subscription-based streaming service after cancelling their account. Jamie submits a formal request through the service's data management portal, asking for the removal of their viewing history, subscription details, and payment information. The streaming service processes the request and initiates the data deletion procedure. However, they retain some information, such as billing records needed for financial reporting and to comply with legal requirements. After completing the deletion process, the service sends a confirmation to Jamie, ensuring that all non-essential data has been removed while retaining only what is necessary for legal compliance.

Right of grievance redressal: Consumers are entitled to use a grievance redressal mechanism provided by a data fiduciary or consent manager for issues related to the handling of their personal data or the exercise of their rights. This is especially important with PbD practices, which may affect data ethics and governance. Consumers must first seek resolution through this mechanism before approaching the Board**.**

Example: Sarah, a data principal, encountered an issue where her request to opt out of promotional emails was ignored by the online retailer ShopP, a data fiduciary. Utilizing the readily available grievance redressal mechanism provided by ShopP, she formally lodged a complaint. ShopP promptly acknowledged her grievance within the required timeframe and addressed the issue by correcting the data handling error and updating her preferences. The swift resolution allowed Sarah to have her rights under the DPDPA respected without needing to escalate the matter to the Data Protection Board.

Right to nominate: Consumers have the right to nominate another individual to exercise their personal data rights in the event of their death or incapacity.[97] Data fiduciaries are required to provide mechanisms for consumers to make such nominations. This ensures that if a consumer is unable to manage their data rights due to mental incapacity or physical infirmity[98], their designated nominee can act on their behalf, upholding their data protection rights as stipulated by the Act and its rules. This provision helps consumers maintain control over their personal data even in situations where they cannot directly manage it.

Example: John, a consumer who has extensive personal data with a financial services provider, wants to ensure that his data rights are protected in case of unforeseen circumstances. He uses the nomination feature provided by the provider to designate his trusted sister, Emily, as his data representative. After John's sudden illness leaves him incapacitated, Emily steps in and exercises John's data rights, ensuring that his personal information is handled according to his preferences. The financial services provider efficiently recognizes Emily's role as the nominated individual, allowing her to manage and protect John's data in line with his instructions.

These rights give consumers unprecedented control over their personal information, ensuring it is accurate, relevant, and used according to their preferences.

I. **Increased Transparency, Stronger Accountability and Trust:**Under the DPDPA, increased transparency and stronger accountability practices have a significant impact on consumers. Data fiduciaries are required to provide clear privacy notices in multiple languages, ensuring that consumers understand how their data is being used. Additionally, the requirement for data fiduciaries to publish contact details for a Data Protection Officer ("**DPO**") or a designated contact person enhances accountability.[99] This framework helps build consumer trust by ensuring that any data-related concerns or complaints can be addressed effectively through established grievance redressal mechanisms. These measures collectively foster greater transparency, accountability, and trust in the management of personal data.

II. **Improved Security of Personal Data:** The DPDPA does not prescribe specific standards for data protection but mandates that data fiduciaries follow general obligations that are designed to safeguard data principals' interests. This approach allows industry-specific standards to evolve based on factors like data sensitivity, risk, and industry nature, which can be more adaptive and practical over time. Currently, reporting requirements for cybersecurity incidents are governed by the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013,[100] and the new directions from CERT-In[101] concerning information security practices. The DPDPA also grants the DPBI authority to mandate urgent corrective actions and investigate breaches. As a result, entities may need to report breaches to both CERT-In and the DPBI and comply with directives from each, potentially leading to duplicative efforts. As a result, consumers benefit from a reduced risk of identity theft and unauthorized use of their financial information, providing them with greater peace of mind.

The absence of an explicit PbD mandate in the DPDPA marks a notable shift from the proactive approach embedded in the GDPR. The lack of a PbD requirement under the DPDPA may lead to a more reactive approach to personal data protection. Organizations might prioritize functionality and development speed over integrating privacy measures from the start, which could result in higher compliance costs and complex retrofitting efforts as privacy issues arise. Without a PbD mandate, consumer trust and confidence may be compromised. Consumers might be more skeptical about the privacy safeguards of products and services if privacy is not integrated from the outset. This shift could necessitate a greater focus on demonstrating regulatory compliance rather than showcasing proactive privacy measures, potentially affecting consumer perceptions and trust.

[97]Id., § 14(1) (Ind.)
[98]Id., § 14(2) (Ind.)
[99]Id., § 8(9) (Ind.)
[100] The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, Gazette of India, (Jan. 16, 2014), available at https://www.cert-in.org.in/PDF/G.S.R_20(E).pdf.
[101] Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology (MeitY), Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet (2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.

In summary, while the DPDPA offers a framework for personal data protection, the lack of a privacy by design requirement emphasizes the need for organizations to be proactive in embedding privacy considerations into their systems. For consumers, this difference highlights the importance of scrutinizing the privacy practices of companies, particularly in the absence of a regulatory mandate that incorporates privacy into the core design of products and services.

Challenges And Opportunities In Implementing Privacy By Design:-

The rapid advancement of digital technologies has made data privacy a paramount global concern. As organizations handle increasing volumes of personal data, the urgency for robust privacy protections has never been greater. PbD presents a proactive strategy, emphasizing the integration of privacy measures into the very core of systems and processes from the outset. PbD is designed to protect user data, drive innovation, and ensure compliance with evolving regulatory requirements. This approach not only addresses the challenges organizations face in implementing PbD but also highlights the opportunities it creates for advancing technology, enhancing customer trust, and navigating the dynamic landscape of data privacy in an interconnected world.

To help organisations gauge their progress, a "PbD Maturity Curve" for emerging economies can be adopted.

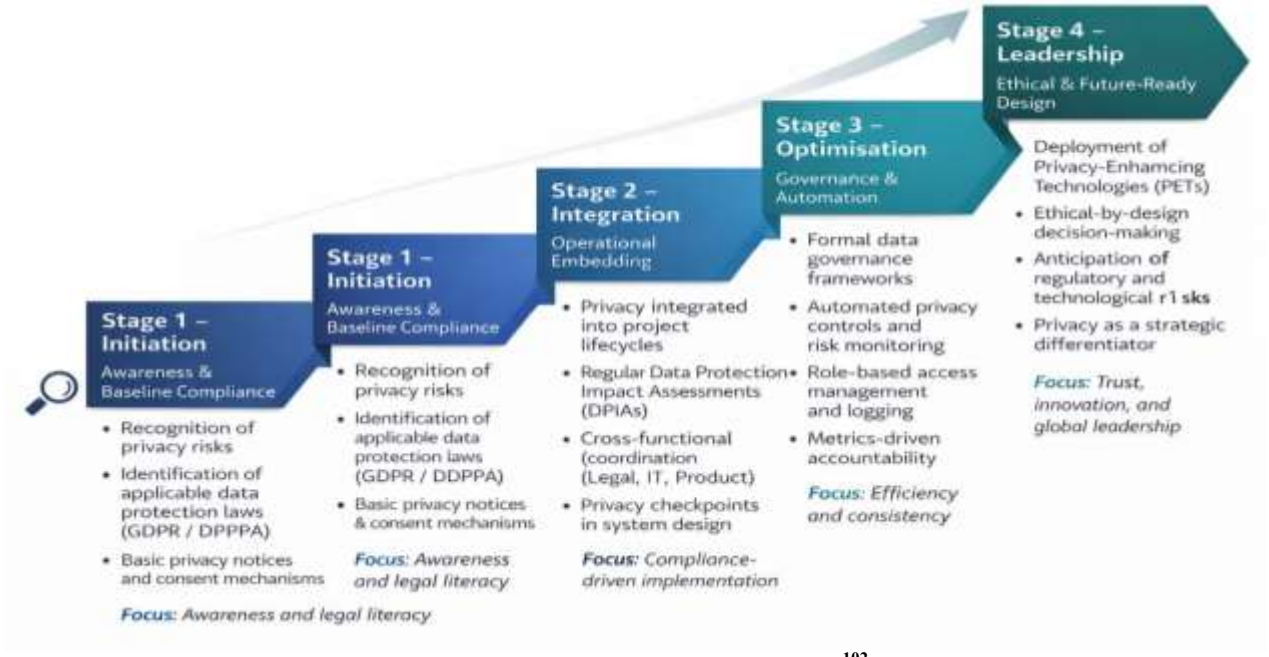

Figure 9 – PbD Maturity Curve for Organisation[102]

Technical Challenges:-

Integration with Existing Systems: Integrating privacy features into legacy systems is a significant technical hurdle. Many organizations still operate on outdated infrastructure that was not designed with modern privacy standards in mind. Retrofitting these systems to comply with PbD principles can necessitate extensive technical modifications and considerable financial investment.

Data Security Measures: Implementing robust data security protocols, such as encryption, anonymization, and secure access controls, is technically demanding. Organizations must ensure that these measures do not compromise system performance or usability while effectively preventing data breaches.

[102] The visual representation of this figure was generated using an AI-assisted design tool based exclusively on an original conceptual framework developed by the Author. The conceptualisation, structure, analytical stages, and legal reasoning embodied in the figure are entirely the Author's own.

Complexity of Data Flows: Managing and safeguarding data across diverse systems and platforms adds another layer of complexity. Organizations must ensure consistent application of privacy measures across all data processing activities, which is challenging in environments with complex data flows.

Operational Challenges:-
Resource Allocation: Implementing PbD requires significant resources, including financial investment, skilled personnel, and time. Organizations must allocate appropriate budgets and human resources to develop and maintain privacy features, conduct DPIAs, and train staff. For example, Small and Medium-sized Enterprises (SMEs) may struggle to allocate the necessary funds and expertise to implement comprehensive privacy measures, leading to potential compliance gaps. These organizations may need to prioritize their privacy investments and explore cost-effective solutions.

Regulatory Compliance: Navigating the regulatory landscape of multiple jurisdictions can be complex and burdensome. Organizations operating internationally must comply with various regulations, each with distinct PbD requirements, leading to increased compliance costs and administrative challenges.

Change Management: Implementing PbD often necessitates substantial changes to organizational processes, culture, and practices. Effectively managing these changes is crucial for successful implementation, particularly in organizations with entrenched practices and resistance to change. For example, transitioning from a reactive to a proactive privacy strategy may face resistance from staff accustomed to traditional methods. Organizations must engage in effective change management, including leadership support and employee training, to foster a culture that prioritizes privacy.

Cultural Barriers:-
Privacy Awareness: In some organizational cultures, privacy may not be prioritized, leading to challenges in embedding a privacy-centric mindset. Organizations need to raise awareness about the importance of PbD and integrate privacy considerations into their corporate values and everyday practices.

Executive Buy-In: Securing buy-in from senior management is essential for the successful implementation of PbD. However, privacy may not always be seen as a strategic priority at the executive level, leading to insufficient support and resource allocation.

Global Compliance Complexities:-
Diverse Regulations: Organizations operating globally must navigate a patchwork of privacy regulations, each with its interpretation of PbD. This regulatory diversity complicates compliance efforts and often requires tailored approaches for different jurisdictions.

Cross-Border Data Transfers: Ensuring compliance with regulations governing cross-border data transfers adds another layer of complexity. Organizations must implement mechanisms to ensure that international data transfers meet the privacy standards required by different jurisdictions.

Opportunities for Innovation:-
Proactive Privacy Measures: Implementing PbD encourages organizations to innovate by developing new technologies and processes that enhance privacy protection. This proactive approach can lead to the creation of advanced privacy solutions and improvements in data handling practices. For example,Companies pioneering privacy-focused technologies, such as differential privacy techniques and secure multi-party computation, can gain a competitive edge by offering advanced privacy features. These innovations address emerging privacy challenges and set new industry standards.

Competitive Advantage: Organizations that effectively implement PbD can differentiate themselves in the market by demonstrating a strong commitment to privacy. This competitive advantage can attract privacy-conscious consumers and partners, leading to increased market share and customer loyalty.

Demand for Enhanced Privacy Controls: Consumers may demand more granular privacy controls, allowing them to manage their data more effectively. Organizations will need to provide users with tools and options to customize their privacy settings in line with their preferences. For example, organizations could develop AI-driven privacy

management platforms that allow users to customize their data preferences at a granular level, with real-time adjustments based on context and usage patterns. These platforms would empower users to manage data access, sharing, and retention dynamically, enhancing compliance with PbD principles while addressing the sophisticated privacy demands of modern consumers.

Enhancing Customer Trust:-

Building Trust: By integrating privacy features into their products and services, organizations can build trust with customers. Transparent privacy practices and effective PbD implementation enhance customer confidence in how their data is managed and protected.

Customer Loyalty: Customers are more likely to remain loyal to organizations that prioritize privacy and data protection. By adhering to PbD principles, organizations can enhance customer retention and build long-term relationships based on trust.

Leveraging Emerging Technologies:-

Artificial Intelligence (AI): AI can facilitate PbD by automating privacy management tasks and performing real-time analysis and monitoring. AI-driven tools help organizations identify and mitigate privacy risks, enhancing overall privacy protection. For example, an advanced AI-driven privacy management systems use machine learning to monitor data processing in real-time, detecting patterns and anomalies that could indicate privacy risks.[103] This enables organizations to quickly address vulnerabilities and ensure adherence to privacy regulations, thereby streamlining compliance and enhancing overall data protection.

Blockchain Technology[104]: Blockchain offers a decentralized approach to data management, enhancing transparency and security. Implementing blockchain for data storage and transactions can support PbD by providing immutable records and ensuring data integrity. For example, blockchain technology can be utilized to create a decentralized, tamper-proof ledger of all data processing activities, including access logs and modifications. Each step of data handling—from collection to processing and sharing—is recorded on an immutable blockchain. This system enables real-time tracking and auditing of data, ensuring that any unauthorized access or changes are immediately visible and traceable. Such a solution enhances compliance with PbD principles by guaranteeing data integrity and providing verifiable evidence of adherence to privacy practices.[105]

Integration with Emerging Trends: PbD will need to adapt to emerging trends, such as the Internet of Things[106] ("**IoT**") and 5G technology[107]. Ensuring that privacy considerations are integrated into these technologies will be crucial for maintaining effective privacy protection[108]. For example, integrating privacy by design into the IoT and 5G technology demands sophisticated strategies to handle the substantial data volumes and real-time processing.[109] For IoT networks, this involves embedding privacy-preserving algorithms directly into devices to anonymize data before it is transmitted, minimizing exposure risks. With 5G, implementing decentralized edge computing can enhance data security by processing sensitive information closer to its source, thus reducing the risk of breaches

[103] Victoria Shutenko, AI Anomaly Detection: Best Tools And Use Cases, TECHMAGIC (May 21, 2024) https://www.techmagic.co/blog/ai-anomaly-detection/.

[104]What is blockchain?, IBM,https://www.ibm.com/topics/blockchain (last visited Sept. 17, 2024).

[105]Blockchain: What It Is, How It Works, Why It Matters, BUILT IN,https://builtin.com/blockchain(last visited Sept. 17, 2024)

[106]Internet of Things, ORACLE, https://www.oracle.com/in/internet-of-things/#:~:text=What%20is%20IoT%3F,and%20systems%20over%20the%20internet (last visited Sept. 17, 2024).

[107]What Is 5G?, CISCO, https://www.cisco.com/c/en/us/solutions/what-is-5g.html#~faqs (last visited Sept. 17, 2024).

[108] Sudeep Srivastava, 5G and IoT: Emerging Technologies with Endless Use Cases, APPINVENTIV. (September 13, 2024), https://appinventiv.com/blog/5g-iot-technology/.

[109]A. K. M. Bahalul Haque et al.,5G AND BEYOND (Springer, 2023), https://doi.org/10.1007/978-981-99-3668-7_11.

during data transmission. Such integration requires designing systems with advanced, context-aware privacy controls that adapt to the increasing data flow and connectivity challenges.

PbD signifies a transformative approach to data protection, shifting privacy from a reactive measure to a fundamental aspect of system development. Despite the significant challenges—ranging from technical and operational difficulties to cultural and regulatory complexities—implementing PbD presents valuable opportunities for innovation and competitive differentiation. Organizations that adopt PbD principles not only align with current and forthcoming privacy regulations but also cultivate stronger customer relationships through enhanced trust and transparency. As technological advancements continue to reshape the landscape, the principles of PbD will be pivotal in developing secure, privacy-focused systems that meet the expectations of an increasingly privacy-conscious society.

Conclusion:-

This in-depth exploration of PbD within the contexts of the GDPR and India's DPDPA underscores its pivotal role in shaping the future of data protection. Both regulatory frameworks emphasize PbD as a cornerstone of modern privacy practices, reflecting a shared global commitment to embedding privacy considerations from the very beginning of data processing activities.The GDPR and DPDPA both highlight PbD as a fundamental principle, mandating that organizations incorporate technical and organisational measures into their design and operational processes. This alignment across jurisdictions signals a unified approach to enhancing data protection, showcasing the importance of integrating privacy into the core of data management practices.The journey towards implementing PbD is fraught with challenges. Organizations encounter various technical, operational, and cultural barriers. Technically, developing and integrating privacy-enhancing technologies can be complex and resource-intensive. Operationally, organizations must adapt their processes and train their workforce to prioritize privacy effectively. Culturally, fostering a privacy-centric mindset within organizations requires a significant shift in attitudes and practices. Despite these challenges, the potential benefits of PbD are substantial. It not only drives innovation and strengthens customer trust but also provides a competitive advantage in an increasingly privacy-conscious market. Emerging technologies such as artificial intelligence and blockchain are particularly valuable, offering innovative solutions to enhance privacy and address evolving risks.

For policymakers, the focus should be on promoting international consistency in PbD standards, offering clear and actionable guidelines to support organizations, and assisting SMEs in their compliance efforts. Collaboration among regulators is essential to streamline and harmonize privacy practices globally, reducing the complexity for businesses operating across borders. Organizations must proactively integrate PbD into their systems, embrace comprehensive data management practices, and nurture a culture that values privacy. Engaging with regulatory authorities and staying informed about evolving privacy requirements are crucial for maintaining compliance and adapting to new challenges.PbD is more than a regulatory requirement; it represents a transformative approach to data protection. By prioritizing proactive privacy measures, PbD shifts the focus from reactive responses to preventive strategies. In an age where digital interactions are ubiquitous and personal data is highly valuable, PbD is crucial for creating a secure and privacy-respecting digital environment.Adopting PbD fosters a culture of trust and accountability, which is essential for maintaining consumer confidence. It enhances organizational resilience against data breaches and privacy risks, contributing to overall security and compliance. As the digital landscape evolves, continuous dialogue and innovation in privacy practices will be vital for addressing emerging challenges and safeguarding individuals' privacy rights.

Looking ahead, Indian regulators should explicitly incorporate Privacy by Design and Privacy by Default into the DPDPA through secondary rules or amendments. DPIAs should be required for all high-risk processing, not just significant data fiduciaries. Sector-specific codes of practice and cross-border transfer mechanisms, akin to standard contractual clauses or binding corporate rules, would align India with global best practices and strengthen individual rights.

To build a secure and privacy-respecting digital future, it is imperative that all stakeholders: regulators, businesses, and technologists, commit to PbD. Regulators should refine and harmonize PbD standards, promote cross-border collaboration, and provide clear guidance to facilitate effective implementation. Businesses need to embed PbD into their systems and processes, adopt comprehensive data management practices, and foster a culture of privacy. Technologists should drive innovation in privacy-enhancing technologies and develop tools that support PbD. By collectively embracing PbD, all stakeholders can contribute to a digital world that not only meets regulatory

requirements but also prioritizes individual privacy, paving the way for a more secure, trustworthy, and privacy-conscious future. This commitment not only fulfils legal obligations but also sets the stage for a future where privacy and security are integral to technological progress and business practices.A comprehensive compliance architecture for Indian organisations should include: (1) Risk classification of data fiduciaries based on data volume and sensitivity; (2) Consent-orchestration platforms integrating consent managers into business workflows; (3) Automated DPIA tools that flag privacy risks in new projects; (4) Unified reporting dashboards to monitor breach notifications and compliance status; and (5) Cross-border transfer registers tracking destinations, safeguards and negative-list notifications. This blueprint operationalises Privacy by Design while ensuring compliance with the DPDP Act and GDPR.