DSCI
PRIVACY
LEADERSHIP FORUM

PRIVACY BY DESIGN

Guidance on Practical Implementation for Businesses

Authors

- Jagannath PV
- Aswathy Asok
- Dwarka Srinath
- Vindhya Vishwanath Kudva

Contributor

- Shivangi Malhotra

Disclaimer

This publication is part of the DSCI Privacy Leadership Forum content series.

The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the views or positions of DSCI. The views expressed by the authors are their own independent expert views and do not reflect their organizational practices or stance.

The information contained herein is for general awareness purposes only. It should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided.

DSCI shall have no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. DSCI disclaims all warranties as to the accuracy, completeness or adequacy of such information.

Foreword

Privacy, as a discipline, has moved forward substantially over the last few years. More so, in terms of the consciousness that is being witnessed across the globe, vis-à-vis treatment being meted out to personal information. Multiple dimensions, facets and nuances of the subject are coming to the fore which is nudging the ecosystem in a direction where Privacy considerations have started taking centre stage.

Organizations are expected to diligently think through, formulate and execute their data handling practices. Several digital economies across the world have been making great strides when it comes to strategizing their Data Protection regimes. Comprehensive legislations anchored on the principles of transparency, accountability and demonstrability are being enacted and entities which are custodians of personal information are working towards streamlining their practices to foster consumer trust and build confidence with the regulatory machinery.

While a good comprehension has started kicking in with regard to the fundamental principles of Privacy, several organizations are still figuring out the most optimal way for carrying out the operationalization of these principles. Lot of organizations are just getting started with their respective journeys. DSCI has been working along with the industry to build those capacities and capabilities that could enable Privacy implementation.

The DSCI Privacy Leadership Forum, an industry effort in this regard, has been set up to lay emphasis on the on ground practical challenges and impediments. The forum, structured in the form of Special Interest Groups (SIGs), is being driven by Privacy leaders and heads of leading organizations, who have pooled in their invaluable experiences, perspectives, and sheer hard work, to produce work products with the hope that the ecosystem finds these documents fruitful and is able to leverage them in the best possible fashion.

These work products are intended to be living documents that keep getting refined and enriched with the critical and constructive feedback from the readers of the said documents.

DSCI would like to express its heartfelt thanks to the members of the SIGs and the Privacy fraternity for their steadfast support to the discipline.

Vinayak Godse
CEO, Data Security Council of India

Table of Contents

1 Introduction 6

2 Theoretical Contours of Privacy by Design 10

3 The 7 Foundational Principles of Privacy by Design 13

4 Practical Implementation of Privacy by Design 16

5 Implementation and Adoption in Business Processes 19

6 Privacy in an Organization’s Operational Activities 25

7 Leveraging Technology to Embed Privacy in IT systems, Platforms, Applications 33

8 Building a Privacy Culture in an Organization 51

9 Conclusion 55

10 References and Additional Reading Material 56

List of Abbreviations

DLP	Data Loss Prevention
DPDPA	Digital Personal Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPB	European Data Protection Board
FTC	Federal Trade Commission (U.S.)
GDPR	General Data Protection Regulation (European Union)
IDTA	International Data Transfer Agreement
PbD	Privacy by Design
PET	Privacy Enhancing Technology
PII	Personally Identifiable Information
SCC	Standard Contractual Clauses
SOP	Standard Operating Procedure
TOMs	Technical and Organizational Measures

1 Introduction

The collection and use of personal and sensitive personal data is only increasing day by day and is expected to grow to more than 180 zettabytes by 2025 owing to the usage of technologies such as social networks, big data, mobile computing, among others. Personal data has become a key asset across the globe, being characterised as the new oil, that should be managed with high responsibility and accountability. However, reports on privacy violations suggest that implementing good data privacy practices and Privacy by Design and default principles are still not the universal norm.

In the context of data protection, it is important to consider both the socio-cultural posture and the technical aspects in securing personal data. In simple terms, data protection can be understood as the ability to exercise control over personal information, maintaining agency over the collection, use, and disclosure of ones personal information. In an organization, each function has a role to play with respect to protection of personal data or Personally Identifiable Information (PII).

Digital technology has dominated data collection over the last many years and has helped collection of massive troves of personal and non-personal data. This typically happens via online purchases, social media, payments transaction with credit cards, digital transfers, digital IDs, surveillance cameras, and several other sources. The extent of digital footprint penetration of an individual makes it important for organizations to process personal data lawfully and by implementing the right measures to process the data securely. Hence, implementing Privacy by Design (PbD) becomes significantly important.

Privacy by Design as a concept was proposed by the Information and Privacy Commissioner of Ontario, Canada, Ann Cavoukian, in the 1990s. Subsequently, it was acknowledged as a component of fundamental privacy protection in 2010 at the annual assembly of International Data Protection and Privacy Commissioners, and it was recognized in 2012 by the US Federal Trade Commission (FTC) as a practice for protecting online privacy. The GDPR has incorporated Privacy by Design and default by obligating controllers to implement appropriate Technical and Organizational Measures (TOMs) both by design and by default. Globally, Privacy by Design is being recognized and adopted across various data privacy regulations.

Europe – GDPR

Article 25 on data protection by design and by default articulates PbD in three key clauses:

i. 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 pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner 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.

ii. The controller shall implement appropriate technical and organizational measures to ensure 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, extent of their processing, period of their storage, and their accessibility. In particular, such measures shall ensure that by default, personal data are not made accessible without the individuals intervention to an indefinite number of natural persons.

iii. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

European Data Protection Board (EDPB) guidelines clarify that TOMs can range from adopting a technical solution to putting in place a process for training on customer data. The guidelines call out some specific examples on handling customer data. However, the guidance does not prescribe which technical measures one must adopt to be able to align with the relevant regulatory norm and Privacy by Design. Invariably, this has resulted in different understandings of the concept and an inconsistent implementation of PbD across organizations.

US – California Consumer Protection Act (CCPA), as amended by Proposition 24

The CCPA, as amended, emphasizes Privacy by Design practices – with specific mentions for business to embed privacy into the design of their processes and IT systems. Mandates such as a clear link for users to opt-out of the sale or share of their data, an option for users to limit the use of their sensitive personal information, and a focus on data minimization all point to Privacy by Design practices.

Brazil – Lei Geral de Protecao de Dados (LGPD)

The LGPD in Brazil requires businesses to have their data processes and systems designed with privacy as the default setting. They also need to be able to demonstrate how privacy has been incorporated into the product or service design to the ANPD, the enforcement body in Brazil.

ISO PbD standard

Recently, the International Organization for Standardization (ISO) has also adopted Privacy by Design as a norm in ISO 31700 framework, which lays down requirements for embedding data protection into consumer products and services.

The ISOs new standard on Privacy by Design includes two parts:

i. ISO 31700-1:2023: High-level requirements for Privacy by Design.

ii. ISO 31700-2:2023: Use cases to help understand these requirements.

By adopting PbD, an organization can:

i. Seamlessly comply with the legal and regulatory requirements of data protection.

ii. Put in a structured approach that ensures all aspects of data protection are adopted and considered.

iii. Implement differentiated products, services, systems, and processes.

iv. Establish privacy as a competitive advantage.

v. Improve the security and efficiency of data processing activities.

vi. Enhance the accountability and transparency of its data processing activities, products, services, systems, and processes.

vii. Avoid the false trade-off between privacy and other objectives, such as security, functionality, or profitability, and instead seek to achieve both.

In India, under the Digital Personal Data Protection Act, 2023 (DPDPA), the Privacy by Design principle is not explicitly stated. However, obligations on data fiduciaries require them to implement appropriate technical and organizational measures to ensure compliance with the Act. Additionally, security safeguards to prevent personal data breaches must also be put in place. It is important to emphasize that implementation of technical and organizational measures would, in effect, entail incorporating several well-recognised Privacy by Design interventions.

Through this working paper, the authors have attempted to offer insight on practically implementing PbD practices for businesses. This working paper briefly explains the theoretical concepts of Privacy by Design and shares an insight into operationalizing Privacy by Design.

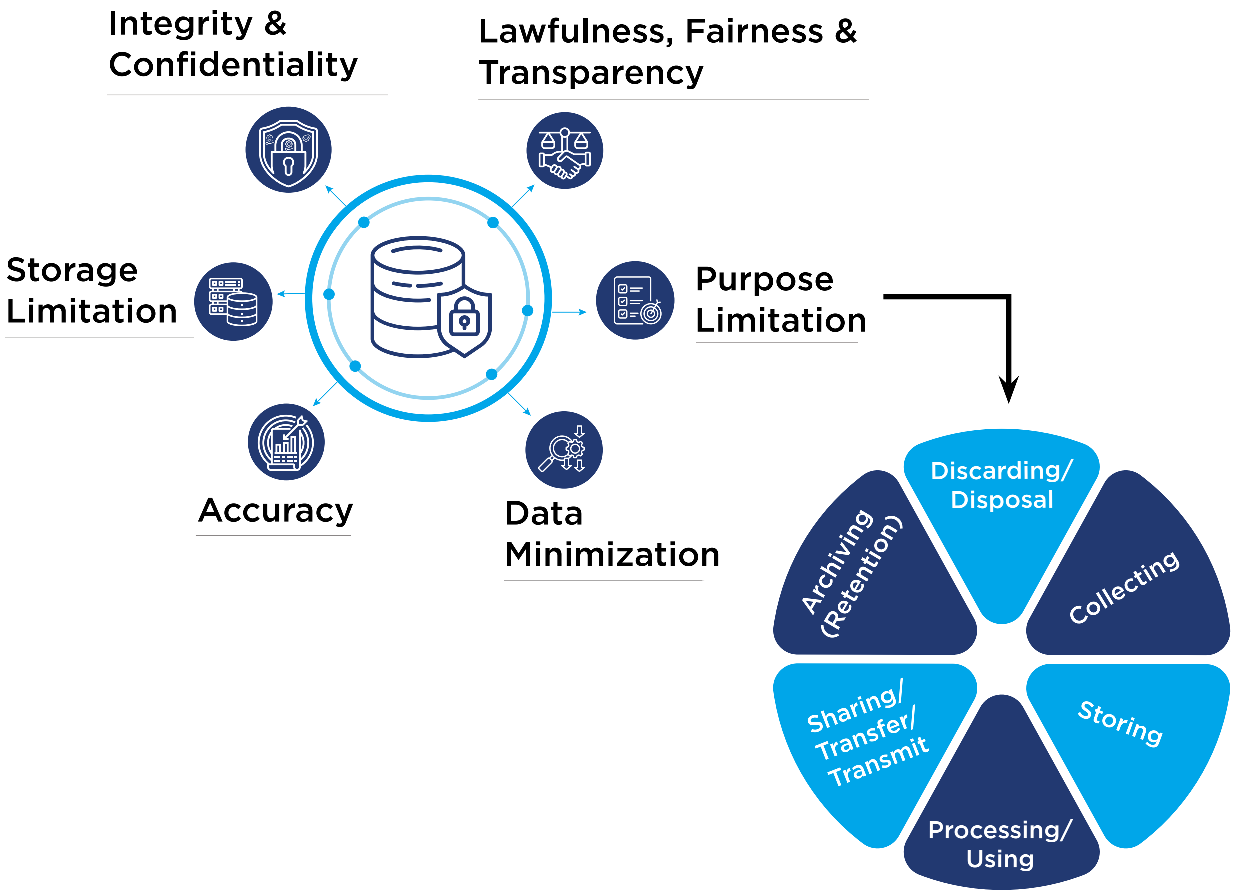
It is important to note that this working paper is envisioned to be a living document. Iterative versions of this document, along with appendices of guidelines applying the methods and approaches detailed here to industry/sector specific target environments, will be released in the future. Among the myriad of privacy-by-design articles and guidance, this paper aims to act as a jurisdiction and sector-agnostic playbook to operationalizing Privacy by Design in the practical world of business and services.

This working paper would be most useful where viewed from the lens of pragmatic implementation of privacy in the end to end lifecycle of data, agnostic of where or who processes such data. Future iterations of this working paper could benefit from a diverse group of practitioners perspectives which would enable metamorphosizing this into industry or sector-specific guidelines.

2 Theoretical Contours of Privacy by Design

The overarching principles in most data privacy laws and regulations are transparency and lawfulness of processing of personal data and protection of the rights and freedoms of data subjects.*

Processing of personal data lawfully and adequately is about aligning with the data processing principles effectively and maintaining this alignment all through the data life cycle from the time of collection of personal data through the disposal of personal data by an organization.



* *The term data subject has been used to refer to individuals who are identifiable in relation to such personal data. It may be read to include inferences to data principals, natural persons, individuals, etc. as called in different data protection laws.*

The foundational principles for processing personal data are explained below.

Lawfulness, Fairness, and Transparency

Process personal data lawfully and fairly in a transparent manner and by letting the data subject know what data you are collecting, the reason for collecting it, manner of processing it and the purposes for which it will be processed.

Purpose Limitation

Specify the purpose for which personal data is being collected and process personal data only for the specified reasons. Any further processing should be done in a manner that is not incompatible with the specified purposes.

Data Minimization

Collect and process only such personal data which is necessary for specified purposes of processing.

Accuracy

Information collected must be kept up to date and steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

Storage Limitation

Store data for only as long as it is required and till the purpose for which it was collected has not been fulfilled. Delete any personal data that is no longer necessary for fulfilling specified purposes, unless there is a legal mandate to retain the data as per applicable laws.

Integrity and Confidentiality

Ensures adequate security of the personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage, using appropriate technical or organizational measures.

So, what is Privacy by Design and what difference does it make to processes and platforms/applications when implemented?

How does it ensure data privacy and security to data subjects?

Data privacy must become an integral part of an organizations objectives, design processes, and operations. Privacy must be embedded into every standard, protocol and process that involves personal data of individuals. To facilitate this, implementing Privacy by Design will help organizations to structure, organize, and adopt ethical practices of data privacy, simultaneously, providing confidence to data subjects and regulatory bodies on processing of personal data.

Privacy by Design

When an organization undertakes an action that involves processing of personal data, such an action must be done with data protection and privacy at the forefront in every stage of the data lifecycle. from data collection to data disposal including processing, storing, sharing, and deleting.

PbD is about embedding privacy into the design of IT systems, operations and business practices upfront, so personal data is processed according to the law and ethically and not as an afterthought.

Adopting PbD helps organizations put in a structured approach that ensures all aspects of data privacy are adopted and considered due course of forming the operational, technical and systemic framework.

Privacy by Default

Once a product or service has been released to the public, it must come with the strictest privacy settings by default, requiring minimal manual intervention from the end user.

For instance, an unticked check box which seeks a customers consent for subscription to marketing/advertisement content exemplifies privacy by default settings. In this case, the customers personal data, by default, is not shared for promotional purposes however they can choose to opt in for the same at any point.

Another example, in the case of social media for instance, may entail setting the default of a users account to be private and requiring an explicit intervention from the user to change the account visibility to public.

3 The 7 Foundational Principles of Privacy by Design

This framework is built on seven foundational principles of Privacy by Design and governed by the data processing principles mentioned in the previous section, all through the data lifecycle.

PbD is based on the conception of privacy as the default modus operandi within the business models of organizations, extending to information technology systems that support data processing, related business processes and practices, and physical and logical design of the channels of communication utilised.

Privacy can be ensured by putting into practice the seven foundational principles as defined by Ann Cavoukian:

i. **Proactive not reactive; preventative not remedial** - This principle requires organizations and actors to proactively anticipate privacy-impacting events before their occurrence and design systems, processes, and infrastructures to minimise privacy risks to data subjects before any damage is caused.

   In brief, PbD avoids **"the policy of rectification"** and anticipates the materialisation of risk. Amongst other things, this involves a clear commitment by the organization, a culture of continuous improvement by all stakeholders, defining and assigning concrete responsibilities, and developing systems and methods for early detection of any privacy-deficient practices.

ii. **Privacy as the default setting** - This principle requires the provision of highest possible levels of privacy protection to a user by default, given the state of available technology. This principle, in practical terms, is based on ensuring data minimisation throughout all stages of data processing. Actionable steps for adherence to this principle would include:

   a. Defining a strict data collection criteria,

   b. Limiting the use of personal data for specified purposes,

   c. Restricting access to personal data in accordance with the "need to know" principle and on a functional basis behind the creation of differentiated access profiles,

d. Defining strict retention policies complemented with operational mechanisms to guarantee compliance,

e. Creation of technological and procedural barriers to prevent unauthorised linking of independent sources of data.

iii. **Privacy embedded into design** - This principle requires organizational thinking to incorporate privacy as an integral and inseparable part of the systems, applications, products and services, as well as the business practices and processes. Some interventions that could operationalise this principle include:

a. Performing risk analysis of the rights and freedoms of persons and when applicable.

b. Performing data protection impact assessments as an integral part of any new processing initiative.

c. Documenting all decisions that are adopted within the organization from a “privacy design thinking” perspective.

iv. **Full functionality: positive-sum, not zero-sum** - The traditional understanding of privacy which gave rise to dichotomies such as privacy vs. usability, privacy vs. functionality, privacy vs. business benefit, and even privacy vs. security, etc. presents a contrived approach in the present day. The goal must be to seek optimal and balanced outcomes with an acceptance for new solutions which are functional, effective and efficient at both business and privacy level.

v. **End-to-end security (full lifecycle protection)** – Another important foundation of Privacy by Design is to ensure privacy protection throughout the lifecycle of data processing. While information security involves the confidentiality, integrity, availability, and resilience of the systems that store personal data, privacy interventions also guarantee unlinkability, transparency and the data subjects capacity for intervention and control in the processing, i.e., intervenability.

Throughout the data lifecycle, each set of operations should be carefully analysed to implement the most adequate measures for information protection, such as pseudonymisation/anonymisation techniques, default encryption, etc.

vi. **Visibility and transparency** - Ensuring visibility and transparency in data processing is essential for an organization to be able to demonstrate accountability before regulators and as a measure of trust before data subjects. Achieving this can involve the adoption of various measures including making data protection policies which govern an organization publicly available, drafting clauses of a privacy notice in manner which is easily accessible and concise to improve the understanding of data subjects, and establishing simple and effective means of communication and grievance redressal for the data subjects.

vii. **Respect for user privacy (keep it user-centric)** - Without forgetting the legitimate interests of the organization with regard to the data processing it performs, the ultimate goal must be to empower the users whose data is processed. This involves designing "user-centric" processes, applications, products, and services, anticipating their needs.

Due regard should be given to the active role of the user in managing their data and in controlling what others do with it. Reiterating the privacy-by-default principle, a users inaction must not imply reduced privacy. Amongst other interventions, this may include implementing privacy settings that are "robust" by default and where users are informed of the consequences and existing risks associated with processing and implementing efficient mechanisms that allow data subjects to exercise their data protection rights.

4 Practical Implementation of Privacy by Design

This working paper articulates the guidance to a practical implementation of PbD effectively into all components of the data life by effectively collaborating "data privacy principles" and the "7 foundational principles of PbD". This is showcased by calling out practical guidance on potential steps that can be taken to ensure privacy is embedded accordingly.

The approach to operationalizing Privacy by Design can be derived from various anchor points, some of which are described below. The most appropriate approach can vary based on the size, scale, complexity and nature of the organization, systems, and stakeholders in scope of the Privacy by Design program:

Business Goal Driven Program

- In this, the primary anchor point is on meeting business objectives while preserving privacy functionalities

Risk Driven Program

- In this approach, risk assessments supported by a selection of privacy controls decide the efficacy of the privacy by design program and the privacy functionalities

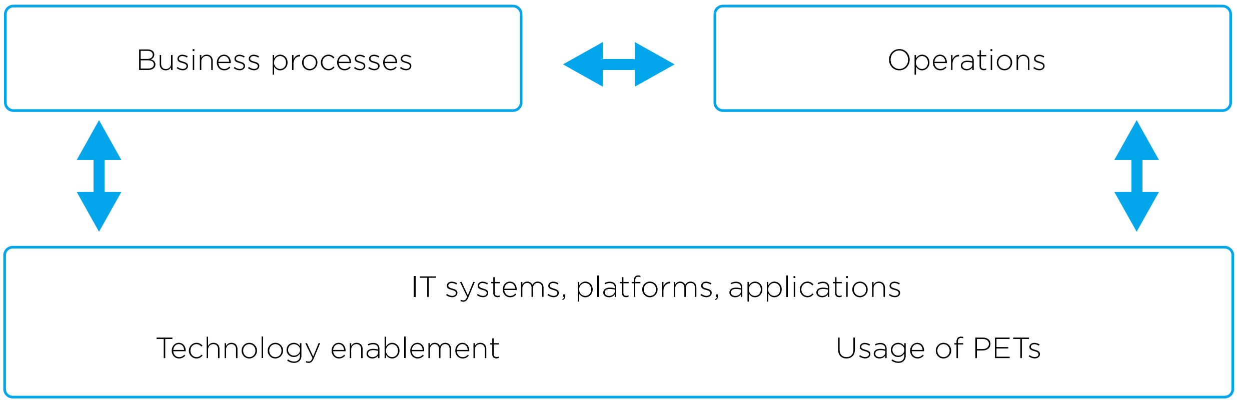
Collaboration Driven Program

- An approach to driving privacy by design outcomes by means of agreements reached between stakeholders is a method that can be followed based on the scale and complexity of the environment the program applies to

In all the above approaches, the full functionality aspect must be ensured with no compromise to any of the principles.

For effective implementation and a holistic view, this guidance suggests implementing Privacy by Design from three different but related vectors:

- Business processes,
- Operations, and
- IT Systems/Applications.



Business Processes

i. While adopting and implementing systems, platforms, and applications that exemplify PbD upfront addresses half the issue. Another important factor is to embed PbD principles into the business processes.

ii. Some examples of such adoption can include building a data inventory, mapping data transfers, identifying data collection points and methods and map to lawful basis, SOPs for incident management, DSR procedures, etc.

Operations

i. Operationalizing the business processes to align with the necessary mandates and guidance under the applicable law is essential. Organizations can achieve this by extending PbD practices and processes into operations. By operationalizing PbD, users can practice privacy embedded practices and processes as a day-to-day BAU procedure.

ii. Examples of adoption of PbD principles in operations include:

  a. Setting up a functional DPO office.

  b. Ensuring a strong and robust governance model is adopted.

  c. Designing and implementing an incident management framework and procedure.

  d. Crafting a robust data privacy training module that covers all roles.

  e. Establishing an effective vendor management process to onboard and offboard vendors, etc.

IT Systems, Platforms, Applications

i. Enabling a standardized PbD culture in an organization can be effectively done by adopting technology solutions. Building and developing systems, platforms and applications that adopt PbD upfront and implement data privacy as a default setting, wherever feasible, plays a key role. This ensures that personal data is processed in line with the principles of processing, assuring that data usage is safe.

ii. Some examples of adoption of PbD principles in IT systems, platforms, and applications can include implementing strong technical controls, usage of PETs, ensuring features such as masking, encryption, drop down list, etc.

The three vectors explained above are now detailed out in the succeeding sections to explain the practical implementation of PbD across business process, operations, and IT systems/platforms/applications.

5 Implementation and Adoption in Business Processes

This chapter calls out various business processes that can be implemented to enable an organization to align with Privacy by Design as a proactive measure.

- Know your sources of data collection
- Map the appropriate lawful basis
- Data inventory. application inventory. processes
- Policies of the privacy framework
- Storage of your personal data
- Data transfers
- Understand processing activities
- Incident management process
- Access management framework
- Data Subject Rights (DSR) process workflow
- Policies and notices
- Contracting
- Awareness and communication
- Risk management process
- Data retention guidelines

Each of the above business processes are detailed below:

Understand all sources of data collection in the organization

i. This is a key component to map and manage the data life cycle of personal data in an organization. Identifying the source of collection, purpose of collection, and purpose of processing accordingly will give businesses an understanding of how and what data is coming into an organization.

ii. Based on this input it will be possible to apply the appropriate lawful basis for processing such data and to understand if such data is being processed according to the applicable data protection law/regulation.

iii. Organizations should ensure every data collection point has a defined traceable audit log. For instance, consent management framework, contracts, applications, etc.

Map the appropriate lawful basis for data processing

i. An organization must be able to attach a lawful basis of processing to every category of personal data it collects and processes. This will help an organization identify if it is collecting such personal data lawfully with the right measures applied and if its processing of personal data is aligned with the law.

   In the absence of this exercise, the organization may not know if it is adequately aligning with the respective data privacy laws and may be at risk of non-compliance because of the absence of a lawful basis for processing.

ii. Some examples can be processing employee data using a contract or consent. marketing data using consent. payroll data using compliance with the law. etc.

Establish a process to know your data - data inventory application inventory processes

i. This is typically done by first listing down all the business enabling processes your organization conducts (both in the roles of a Controller/Fiduciary and Processor)

   a. Examples of Controller may be HR, Payroll, Marketing etc.

   b. Examples of Processor may be customer projects, BPO, etc.

ii. While establishing the data inventory, it is apt to also define the data lifecycle as follows:

   a. Source of the data

   b. Collection aspects

   c. Storage aspects

   d. Distribution/sharing/transferring aspects

e. Access aspects

f. Retention aspects

g. Deletion aspects

Implement the relevant policies of the privacy framework

Clearly draw out and list down all the policies of the internal privacy framework that the organization needs and wants to implement and how it impacts the organization.

Some examples may include privacy notices, data retention policy, data subject rights management policy, incident management policy. etc.

Know the storage of your personal data

i. Understanding storage of personal data is relevant for several reasons:

   a. Application of appropriate technical and organizational measures.

   b. Ability to understand and make decisions about any jurisdiction-specific considerations.

   c. Ability to ensure that adequate protection is provided to personal data.

   d. Evaluate the need for any jurisdiction level transfer mechanisms.

ii. Some examples can be additional security measures, implementing adequate transfer tools like the SCCs, ensuring that data is not stored in restricted list of jurisdictions, etc.

Understand data transfers

i. Organizations processing personal data from different jurisdictions will need to have a nuanced understanding of legal expectations in each jurisdiction to ensure that data transfers are managed in line with the laws.

ii. Organizations must establish the appropriate transfer mechanisms/tools/contractual measures for lawful transfers.

   Some examples are EU SCCs, UK IDTA, China SCCs, prohibition on transfers to restricted jurisdictions under the DPDPA, including Singapore and Australia transfer nuances into contract, etc.

iii. Conduct transfer impact assessments to understand the exposure of personal data in the jurisdiction in which it is being processed.

iv. Ensure technology and operational supplementary measures are incorporated.

v. Ensure adequate and appropriate processes are put together and applicable localization norms are managed effectively.

Understand processing activities

i. Put together a Data Protection Impact Assessment (DPIA) procedure. Decide the criteria based on which the organization would like to conduct an impact assessment. Correspondingly, maintain the Records of Processing Activities (ROPA). The criteria for deciding whether or not a DPIA is required can be a risk-based criteria, volume-based criteria, or sensitivity-based criteria etc.

ii. This process helps an organization understand the activities it performs on the different kinds of data it collects and processes. Resultantly, this process also helps organizations develop an understanding of the nature and extent of risk undertaken by them in processing such personal data.

Define a robust incident management process

i. The objective of the incident management process must be to attend to the incident without undue delay and focus on restoring operations in minimal time and minimize impact on business operations.

ii. Data breach/incident accountability has become a crucial area for organizations and directly impacts and organizations reputation.

iii. Defining a robust incident management framework will help organizations take quick and effective actions involving relevant stakeholders.

Implement an effective access management framework

i. It is important to define upfront which group of personnel must have access to the personal data being processed, which will be implemented into the operational aspects of PbD.

ii. The approval mechanisms for effective identity and access management should be clearly laid down.

iii. To enable this, organizations should consider adopting a user identity solution that uniquely identifies people and systems.

Design the Data Subject Rights (DSR) process workflow and fulfilment approach

i. Data subject access rights are at the core of any data protection regulation. These rights enable data subjects to access information about personal data the organization is processing about them, request erasure, modification, updating, etc.

ii. Effective DSR processing exemplifies how well an organization knows what data it holds about an individual and how privacy focused is the organization.

iii. With timelines to fulfill a DSR being based on jurisdiction and applicable laws, it is important an organization implements a process that can be easily understood and followed with clear responsibilities and task a specified point of contact to help the organizations in fulfilling a DSR request.

Implement policies and notices ensuring transparency, fairness, and clarity

i. Clearly call out at what points of data collection, what type of notice/consent is to be provided to the data subject. If consent is opted, ensure it is recorded clearly and can be traced back.

ii. Adopt a guidance chart that helps organizations clearly define the different data collections points against the respective lawful basis and respective notices to be shared.

Ensure effective contracting is implemented and understand data transfers

i. Establish standardized templates to ensure personal data shared with or received from third parties are processed with adequate and stringent guidelines. Some key elements of a data processing agreement are: adherence with the law. lawful collection of data. data controller obligations. data processor obligations. data subject rights management. incident reporting and response. reporting of complains. maintaining records of processing. training and awareness. technical and organizational measures. sub-processing. data security. audits. prior consultation. risk assessment. deletion and return of data. restriction on transfers. regulatory inquiries. details of processing. indemnity and liability. and termination.

ii. Understand data transfers being undertaken on multiple fronts. internal and external, intra company and inter company, with vendors and with customers. The relevant contracts should address elements such as processing location, storage location, access location, transfer location etc.

iii. Some data transfers have restrictions and most have contractual nuances to consider (like the SCCs). Build templates that will accommodate these transfers.

iv. Develop a guidance document articulating the respective template to be used for the appropriate transfer that will be performed. For example, developing a contract template for transfer of personal data from a data controller to data processor for an organizations vendors processing the organizations employees personal data. or a template for transfer of personal data from a processor to sub processor for subcontracting vendors etc.

Define a continuous awareness and communication plan

i. Awareness building to highlight the seriousness and importance of processing personal data as per the law is every individuals responsibility. This can be established only by bringing in awareness and continually reminding personnel of their obligations and responsibility.

Articulate a comprehensive risk management process

i. Build a clear, simple, and robust risk management framework that includes risk identification, risk analysis, risk evaluation, risk treatment, risk communication, risk monitoring and review, risk governance, risk closure/acceptance.

ii. As a result of this process, organizations will be able to understand, accept and mitigate risks effectively.

Define data retention policies and guidelines

i. To align with the principle of storage limitation, organizations must put together data retention policies and guidelines. Primarily organizations must ensure they get into the practice of deleting data when no longer needed.

ii. If the personal data is no longer being processed, or if it is outdated, or a sectoral law mandates its deletion, such data must be deleted. Alternatively, it is also important to consider all legal mandates which may require retention of personal data for a minimum specified period.

iii. In the absence of a sectoral law or any other applicable regulation, the organization must take a rational approach on how long it wants to process such personal data and the lawful grounds of processing.

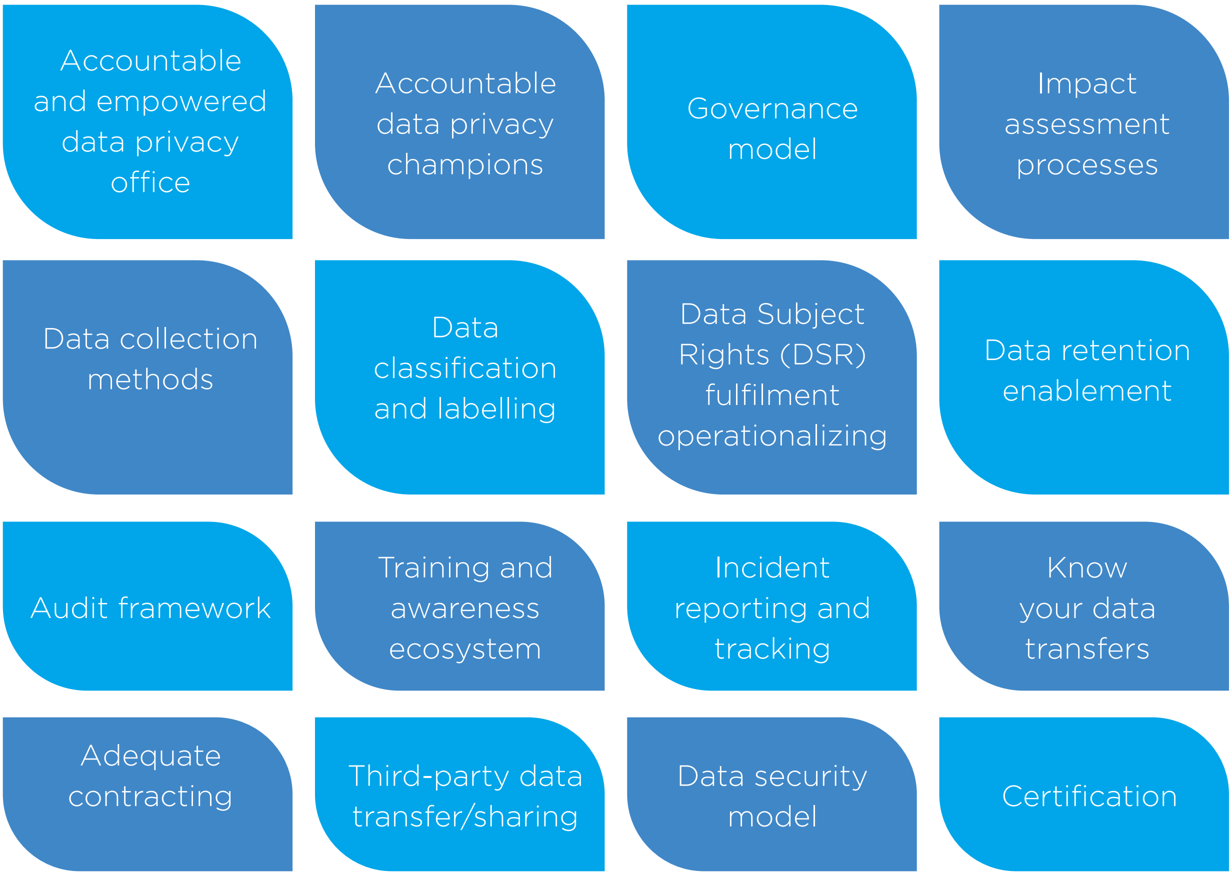
iv. After considering the above-mentioned factors, organizations should aim to define a timeline after which such data deletion process must be commenced.

v. In defining the data retention policies and guidelines, organizations should factor in a legal hold for any data retention. For instance, there may be a legal obligation to retain a specific data set for more than the prescribed timeline because of a legal claim, pending litigation etc. In the process of deletion of unwarranted personal data, the organization must ensure that such data is retained.

6 Privacy in an Organization's Operational Activities

This working paper refers to operationalization as a collection of activities that use Privacy by Design, data protection regulations principles and information available from business processes and stakeholders to effectively select functional capabilities that are used throughout the lifecycle of personal data in processes, while also ensuring alignment to policies and regulations – directly and indirectly governing personal data.

The following section of this whitepaper describes the salient steps in operationalizing a Privacy by Design program irrespective of the approach chosen. For example, putting together an ecosystem, importance of implementing tools and techniques that can help a business process achieve its objectives, etc.



Accountable and empowered data privacy office

Accountable data privacy champions

Governance model

Impact assessment processes

Data collection methods

Data classification and labelling

Data Subject Rights (DSR) fulfilment operationalizing

Data retention enablement

Audit framework

Training and awareness ecosystem

Incident reporting and tracking

Know your data transfers

Adequate contracting

Third-party data transfer/sharing

Data security model

Certification

An accountable and empowered data privacy office

i. An organization must invest in appointing accountable personnel who are capable of understanding and interpreting data privacy laws, defining the organizations data privacy and protection posture, and implementing a robust data privacy framework for processing and protecting personal data.

ii. Organizational support must be provided to the appointed personnel from the highest level to be able to form a governing body that reviews data processing and protection on a regular basis.

Assign accountable data privacy SPOCs/champions

To help the data privacy office implement an effective Privacy by Design culture, the organization must identify accountable stakeholders who will help implement, fulfil, run, and help govern the data privacy and protection obligations across business processes, operations and technology.

Adopt a governance model

For operationalizing an effective Privacy by Design culture and framework, it is important for an organization to measure, update, and govern its data privacy and protection framework on a regular basis. The governance model must ensure it is visible to the highest-level decision makers so actions can be made promptly and effectively.

Perform DPIA and formulate ROPA as per defined criteria

i. This will be one of the primary inputs to the principles of processing.

ii. This process helps an organization understand the activities it performs on the different kinds of data it collects and processes and if such action is in line with the principles of processing personal data.

Manage data collection methods and tools

i. Identify all data collection points.

ii. Map every collection point to the appropriate lawful basis as per the respective privacy law.

iii. Draft a lawful basis framework for every data collection point so to ensure the personal data is aligned with the respective privacy principles and lawful basis all through its data lifecycle.

iv. Implement the appropriate process workflow for every personal data collection point and map the same by adopting a technology/application or a tool for effective management.

This may entail, amongst other things, the following:

a. Consent management tools/consent management module in the platform.

b. Publishing the right notice to the right audience.

c. Aligning an adequate cookie preference management based on the jurisdiction or aligning it with the standards under the strictest jurisdiction.

d. Third party data collection methodology/process flow.

e. Establishing an effective data subject rights management platform.

f. Implementing adequate contractual arrangements to ensure all data privacy obligations are passed to the responsible data processor.

Facilitate data classification and labelling

To manage data exposure, it is important that the personnel who are processing personal data familiar with measures of data protection. Methodology such as data classification and labelling can be adopted. Data classification and labeling can be enabled using tool-based guidance, tool-based implementation, manual implementation via user intervention. This will ensure an individual or a system processing personal data understands the sensitivity of the data being processed.

Ensure Data Subject Rights (DSR) fulfilment is socialized and adhered to as per the defined process

i. Established a centralized process so all DSRs are managed in one place.

ii. Define SOPs and increase organizational awareness of the process to be followed.

iii. Clarify timelines for DSR response and ensure adherence to the same.

iv. Ensure the processes are monitored and outcome is reported.

Data retention/deletion enablement – policy and practice

i. Ensure a retention policy is drafted and agreed upon amongst all business functions.

ii. In line with the principles of data minimization and storage limitation, an organization must only retain data it really needs, and which is necessary for aligning with a statutory obligation.

iii. The ideal approach to data retention is to implement tools to facilitate this exercise at the master level. Any action on the master record triggers the act of deletion on other applications/databases containing the same data point.

The following considerations should be kept in mind:

a. It is important to have the entire inventory of personal data in the organization.

b. Personal data retention will also need to apply to unstructured data. Such data can be found on shared drives, individual servers, documents, individual assets etc.

c. To adhere to effective storage practices, organizations must adopt a practice of storing in enterprise repositories that are secure and access controlled. This will likely make locating such data easier and operationalizing data deletion will be facilitated along with the retention process.

iv. Automated data retention guidelines can help streamline the process flow. Prior to defining any deletion process, the organization must check for any legal obligation to keep this data set for more than the prescribed timeline, for instance due to an ongoing litigation.

Establish an audit framework for both internal and external audits

A clear action plan must be facilitated to ensure that any audit findings, from regulatory compliance, process compliance, or technology compliance can be acted upon in the stipulated timeline.

Implementing a continuous training and awareness ecosystem

Individuals processing and providing personal data must be aware of data privacy norms and understand their obligation while processing personal data that the organization collects.

This can be achieved via different means:

- **Online annual training**
- **Department based awareness**
- **Role based training**
- **Communication fliers, mailers**
- **Incident based training**

Incident reporting and tracking

A data breach is a security incident where sensitive, confidential, or otherwise protected data has been accessed/lost/disclosed in an unauthorized manner. Such incidents/data breaches have the possibility of compromising personal health data, personally identifiable information, intellectual property, confidential information, or trade secrets.

With significant implications for an organizations reputation and regulatory fines, it is very important an organization establishes and operationalizes an incident management process, awareness, intimating the right stakeholders, mitigate and train its stakeholders at all levels.

The operationalized process must be able to proactively identify and/or mitigate a data exposure/data breach/data incident so that the relevant stakeholder can be made aware and appropriate action can be taken at the relevant time. An organization must be well equipped with the following:

i. The ability to identify the incident and report the incident with relevant details.

ii. Based on the identification, the responsible stakeholder must be able to investigate the incident, its cause, scope of impact and influence and impacted/ affected data.

iii. Data incidents have a key component of regulatory notifications. As a result, an assessment must be done against the respective regulatory norms to decide whether the breach is notifiable, and the jurisdictions in which the impact exists. As a result, assessing the incident risks and its impact is highly critical.

iv. The process must provide guidance on involving the right teams and stakeholders that are probably impacted individuals/functions.

v. All relevant stakeholders must be a part of the remediation and prevention processes. The learnings from the identification and remediation of the breach must be taken into the continuous improvement plan for both data security and data privacy.

vi. It is important to also emphasize on third-party contractual obligations for upstream and downstream impacts as the incident can have a ripple effect for which the data controller will be the key accountable party.

Data transfers are crucial in data privacy regulations

Some regulations mandate clear guidelines and tools of transfer whereas certain others rely on strong controls and contracts. Its therefore important to map the data transfers being undertaken by an organization and align accordingly with the tools of transfer (e.g. on-premise/ cloud).

i. Several regulations across the globe mandate or guide aspects related to data transfers for personal data being transferred/accessed outside their jurisdiction. This will involve technical measures to be taken, contractual measures to be considered and process measures to be implemented.

ii. Some examples are:

    a. European data transfers

    b. United Kingdom data transfers

    c. USA with regard to health data/PHI

d. China - SCCs and data transfers

e. Argentina

f. Saudi Arabia

g. India

iii. Establish a strong contract management process that will include the nuances of your data transfers and its respective obligations transferred to data processors and sub processors.

iv. Conduct transfer impact assessments to understand the implications of other laws on the data being transferred.

Operationalize adequate contracting

This is important to ensure that all data privacy obligations are passed to the responsible data processor. It is important for organizations to identify a single owner in the process flow who will be responsible and can hold the relevant stakeholders accountable.

i. This can be applicable to an organizations contracts with third parties or to its customers.

ii. Define adequate technical measures that third parties and customers must implement to process data or enable processing of personal data securely minimizing the data exposure.

Establish a strong control of third-party data transfer/sharing and deletion

i. Establish an effective vendor onboarding and offboarding process that comprises of assessing the data privacy practices of a vendor/third party organization. This process must be embedded as a default alongside the procurement or onboarding process flow.

ii. Define the obligations of the third party for the data being processed via effective contracts. Reference may be drawn from EU SCC Annex 1 – "Personal data processing annex", to arrive at mutual understanding and consensus between the vendor and the respective business on the data being processed by the third party.

iii. Identify technical measures expected to be implemented by the third party.

iv. Evaluate the adherence to data privacy obligations of third parties and its implemented technical measures.

v. For third party transfers, take the relevant measures to transfer data in a secure and protected manner and minimize data exposure.

vi. For transfers from your customer organization to your organization mandate relevant measures you expect the customer to take before enabling transfer/ access of data from your environment in a secure and protected manner and minimize data exposure.

Establish an effective data security model with the CISO

i. The privacy office should collaborate intensively with the IT function and the CISO function.

ii. Guidance from the privacy office on processing personal data must be implemented by the IT and CISO functions to ensure the privacy posture of the organization is technically elevated and in line with the law. This may be applicable to:

a. Application development

b. Employee monitoring and data loss prevention

c. Encryption

d. Anonymization

iii. Embed a process to assess data privacy controls and adoption at the design phase of any application or process and pass it down through implementation and support.

This approach will ensure the organization adopts a proactive measure to embed data privacy nuances and controls upfront and hence provides confidence that its systems and processes are built to manage personal data securely and adhering with the law.

Adopt a data privacy related certification

i. Audit the privacy posture of the organization.

ii. Validate controls implemented by the organization.

iii. Check the personal data collection and processing points.

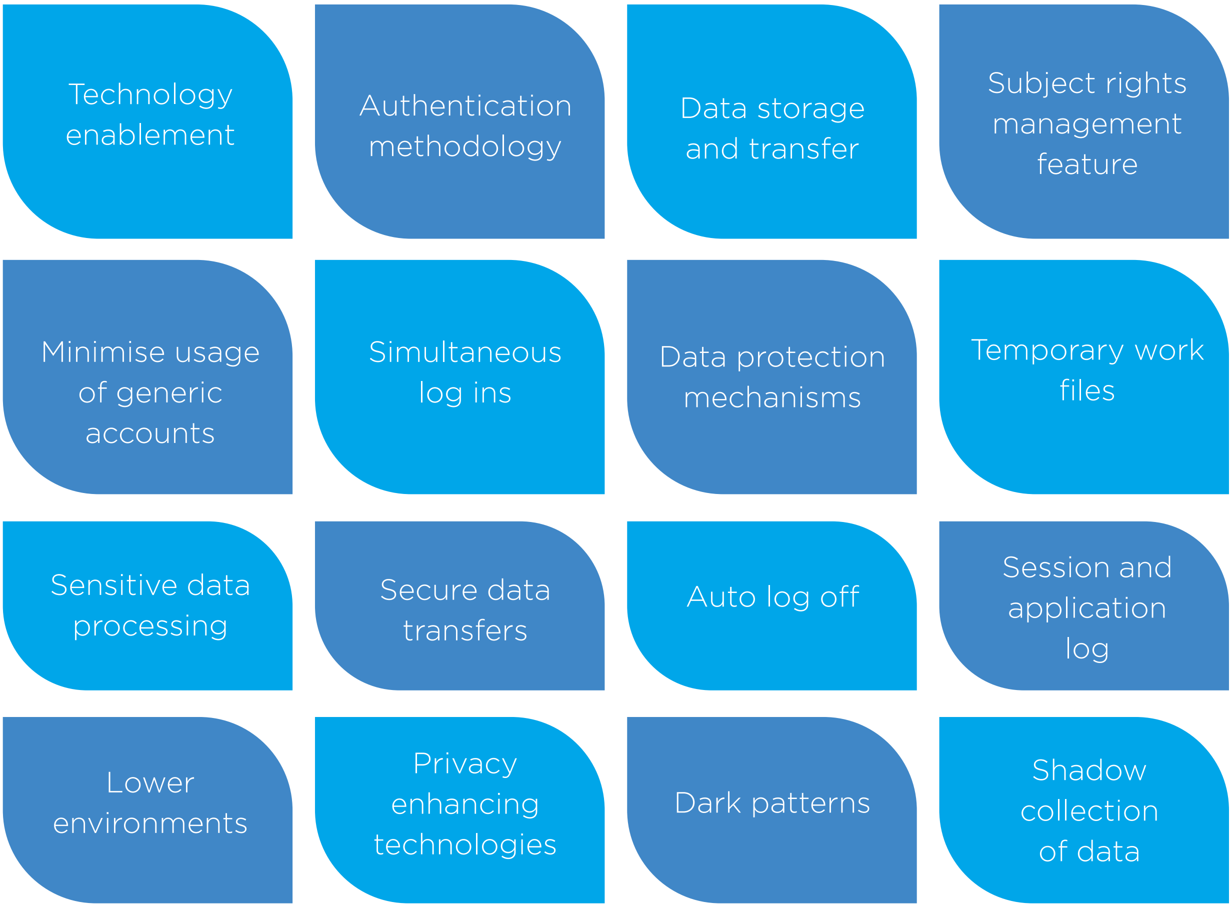
iv. Be up to date on any enhancements to the law and processing operations.

Adoption of Privacy by Design elements in the operational activities of the organization can demonstrate its ability to secure and protect both its data and its customers data. Such a demonstrable ability can also play out as a competitive advantage.

7 Leveraging Technology to Embed Privacy in IT systems, Platforms, Applications

7.1 Technology enablement and adoption

Having discussed implementing/adopting PbD into business processes and then operationalizing PbD to build a PbD culture in an organization, this section provides overview on using technology and technical means to facilitate adoption of PbD to ensure that the means of achieving PbD are consistent and person independent. The following sub-sections provide an insight into how technology may be used for achieving an effective privacy posture into an organizations IT systems, platforms, processes, and applications.



Technology enablement

Authentication methodology

Data storage and transfer

Subject rights management feature

Minimise usage of generic accounts

Simultaneous log ins

Data protection mechanisms

Temporary work files

Sensitive data processing

Secure data transfers

Auto log off

Session and application log

Lower environments

Privacy enhancing technologies

Dark patterns

Shadow collection of data

An effective Privacy by Design alignment is enabled with technology and adopting PETs

First, lets explore how technology can facilitate alignment with PbD, followed by how adopting PETs can help organizations strengthen their privacy posture and embed PbD into their culture. Let us start by addressing the adoption of the principles of processing.

Principles of processing are the backbone of all data privacy regulations/law. Aligning with principles of processing personal data ensures an organization is processing personal data in line with data privacy laws. These principles encompass lawfulness, fairness and transparency, data minimization, purpose limitation, storage limitation, accuracy, maintaining integrity and confidentiality, and accountability.

These principles must be engrained into the entire data life cycle of an organizations data processing. from data collection, processing, access, sharing to disposal. The same must be adhered to all thought the development and deployment of any process/application.

i. Lawfulness, Fairness, and Transparency

a. Decide the appropriate lawful basis. Provide a notice articulating the purpose of processing. Take explicit granular consent. Implement granular consent. Build the ability to opt out in a granular way.

b. For customer-facing applications, build applications with the ability to showcase a notice and integrate with a consent management system to be able to take and withdraw consent effectively.

ii. Data Minimization

Collect only what you need for the specified purpose. A review by the technical and business teams must ensure this check is performed. For instance, in an event registration page sharing contact numbers should be voluntary, avoid collection of national IDs at the time of job application, avoid collection of passport details after conclusion of employment. location and device data should not be accessed on phones on downloading an app. IP address/Mac address should not be collected where not required.

iii. Purpose Limitation

Information collected must be used for the purpose it was collected for, and for which the data subject was informed at the time of collection. If it needs to be used for other purposes, it must be done only with the consent of the person concerned or if authorized by law. Ensure effective access controls are put together and evaluate when any upstream applications are being built. If yes, ensure the purpose is validated and managed accordingly.

iv. Storage Limitation

a. Personal data must be stored only for the time it is necessary for the purpose. Ensure the data is not accessible to an indefinite number of people. If data needs to be shared, share it securely, for example, by utilizing end to end encryption, https, etc.

b. Determine the storage period with the help of a defined retention policy.

c. Implement automated methods for erasing unnecessary and outdated data. Adoption of adequate APIs is necessary to ensure that upstream and downstream applications also implement the action of deletion or erasure.

d. Enable automated means to implement any legal holds on personal data.

e. If data needs to be stored beyond retention, for statistical purposes implement appropriate measures such as anonymization so the data cannot be identified.

f. Collection of browsing data on user device should be minimized. Use of session cookies should be preferred over persistent cookies, clearly define an expiry date for cookies.

v. Accuracy

a. Provide a platform accessible to the data subject for facilitating accuracy of the personal data you process about them. This platform could be an application or a portal or an email ID to reach out to.

b. This can entail either a platform directly accessible by the user empowering them to modify/correct their personal data or it can be a DSR portal/interface that collects this request and then forwards it to the fulfilling team.

vi. Integrity and Confidentiality

Implement roles and right permissions. multi-factor authentication. encryption. access keys. strong password policies. restrict users on failed attempts. store users credentials using an electronic hash of the password. session termination. conduct periodic tests for possible vulnerabilities.

Use strong authentication methodology to prevent unauthorized access

i. Define a strong password policy.

ii. Use solutions like multifactor authentication for more secure access.

iii. Avoid using social media logins.

iv. Adopt secure single sign on mechanisms.

v. Avoid providing the ability to create a generic ID in production environments.

vi. Ensure default user-IDs and passwords are changed on first sign on.

vii. Force password expiration and prevent users from reusing a password.

viii. Implement forced lockout of application.

ix. User-IDs utilized for privileged access should be kept separate from the normal user-IDs that are used for performing regular business operations.

Understand data storage and transfer, adopt adequate tools of transfer

i. Understand jurisdictions of data collection.

ii. Map out the jurisdictions of data storage.

iii. Identify jurisdictions where data is being transferred or shared.

iv. Choose storage locations after assessing available tools of transfer.

v. Ensure the adequate contracts are put together to enable the above mentioned interventions.

vi. Implement appropriate security controls and TOMs.

Build in data subject rights management feature into applications by default

The application being developed should facilitate features that enable the DSR workflow. Alternatively, the DSR workflow can be enabled via an API. Building/ embedding DSR workflows into applications will help manage any relational/up flow/ downflow workflows effectively without missing out on any data subject requests and will facilitate a seamless transition of data.

Minimize usage of generic accounts

i. It is not a good practice to use generic accounts in production environments. This will limit the ability to have an effective audit log/trail of the users accessing systems and data.

ii. Generic accounts will also provide an avenue for more than one individual to know the password and more chances of misuse.

iii. By not using generic accounts we can demonstrate which specific individual accessed the system with adequate time stamps, hence providing the ability to monitor access.

Validate simultaneous log ins

It is important to validate simultaneous log ins because it can result in the increasing ability of unauthorized individuals log on to an environment at the same time.

Implementing data protection mechanisms is key

In an environment processing confidential/sensitive data, implement strong security controls such as but not limited to:

i. Data classification

ii. Data labeling

iii. An effective Data Loss Prevention (DLP) solution across the corporate network and end points to monitor data moving from endpoint systems and email.

iv. Applicable vulnerability management

v. System hygiene

vi. Data destruction controls/systems

Deletion of temporary work files created in a session

Once the session ends, such temporary files should be deleted. This will avoid unnecessary exposure of data which can compromise privacy protection.

Adopt secure data transfers internally and externally

Secure data transfer can not only ensure a safe channel but also ensure access is restricted to authorized users only. Some examples of secure data transfers are:

i. SFTP

ii. HTTPS

iii. Upload directly onto vendor systems

iv. API interface

v. Encrypted password protected files

vi. Minimize sharing data over emails

Implement auto log off feature

Enabling auto log-off when the application is not in use, in the process of development, may mitigate risks such as hacking or compromise of an account, theft of content in a device/application getting stolen, network infiltration, or identity impersonation.

Ensure logs do not contain sensitive data

Logging is important to be able to debug, or attend to an incident, and for forensic evidence. But logging sensitive data is not advised as it impacts privacy of individuals, and also increases the potential for data exposure. One of the ways of avoiding logging personal data is to either mask/encrypt such information or even more effectively log a reference via tokenization. With tokenization, you exchange sensitive data with a token.

Data in lower environments

Ensure data in lower environments are never a replica of production data irrespective of its age. Old data is also real data. Use synthetic data or invest in a pseudonymization tool to either fabricate data or pseudonymize data securely.

Implement Privacy Enhancing Technologies (PETs)

Examples include cookie preference management, cookie walls, etc. for more controlled management of data processing.

i. Cookie laws across the globe are increasingly stringent and websites are being monitored to check on compliance.

ii. Implement cookie scanning technologies. This will help identify many cookies that are not classified manually or are introduced by a third party.

Ensure dark patterns are not implemented into applications

Dark patterns are interfaces or deceptive user experience that mislead users into doing something or performing actions that they didnt intend to. They can range from subtle omissions to outright lies. Implementing dark patterns can attract regulatory investigations and related fines. A few examples of dark patterns are:

i. Making it difficult for users to withdraw consent or cancel a subscription to a service.

ii. Use of deceptive patterns in subscription forcing auto-renewal practices.

iii. Adding an unauthorized fee for services, without user knowledge or consent.

iv. Forcing users into providing access to additional data such as their address book/contact list

Shadow collection/data can be a significant threat to data exposure/leakage

Shadow data is the data that is copied to other sources or backed up and may not be governed on a regular basis nor kept up-to-date by the organizations security/IT department. Illustrative examples of shadow collection include:

i. Copying production databases that are not being secured- like in a test environment, or an unmanaged backup or abandoned databases after a contract termination with a vendor.

ii. Setting up new data storage assets in the cloud, without consultation with the IT department, thereby increasing the probability of data exposure.

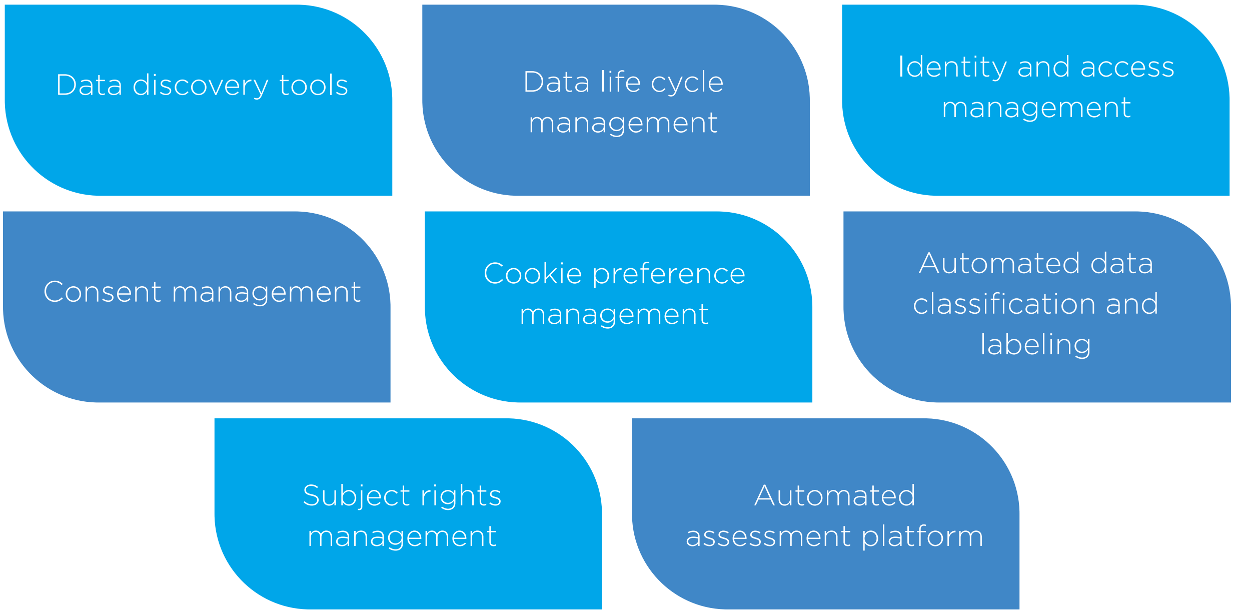
iii. Storing data in platforms like a public/personal GitHub account.

iv. Unprotected Data lakes/analytics pipeline.

Enable audit trail

Determine the timeline based on the organization policies. This will help in carrying out data audits to audit/log all actions on the personal data. It should have an easy extraction design and should also allow time travel requests.

7.2 Adoption of privacy management tools


Data discovery tools
Data life cycle management
Identity and access management
Consent management
Cookie preference management
Automated data classification and labeling
Subject rights management
Automated assessment platform

To manage and govern the data privacy posture of an organization it is best done by investing into privacy management/GRC tools. These tools will facilitate effective governance of the data privacy framework. Using such tools will also help in accurate and transparent representation and reporting of the operational parameters of a data privacy framework. Some of these interventions are examined below.

Data discovery tools

i. Data discovery tools help an organization understand where data resides in an environment.

   a. These tools can help develop a data catalog so it can provide a reliable record of where the data is located and its precise classification. To protect the data effectively, analytics systems should know the classifications of the source data so that the systems can govern the data according to business needs.

b. Investing in data discovery tools enables the discovery of both structured and unstructured data. Organizations may still follow a step-by-step plan and begin with structured data followed by unstructured data.

c. Discovery tools will scan and identify across different environments such as cloud, on-premises, individual assets, public cloud, collaboration platforms, other organizations, applications, storage, on temporary spaces, etc.

ii. Document a data inventory and application inventory to be able to map personal data being processed in the organization.

iii. Draw a map of the entire data lifecycle of every data element/category of data.

Data life cycle management

It is an approach to manage data from collection through data destruction. Using a PET will help this process to identify and manage effectively and seamlessly the following aspects:

i. How do you collect data and on what basis?

ii. Who has access to it and how is the access managed?

iii. Who is it shared with, and the aspects considered for sharing?

iv. How is it kept secure? What are the technical and organizational measures considered?

v. Where is it stored? Both live/production data and back up data. copies of the data.

vi. Where is it transferred? (Internal and external transfers to understand how many copies of such data are being created and stored)

vii. How is it discarded/disposed? (Internal and external – what mechanisms and what tools are being used to detect and dispose?)

Identity management systems and access control

i. Solutions must be able to uniquely identify the people or systems to control access effectively. For example, the workload should be able to tell who accessed the data by looking at the user identifiers.

ii. Data owners should be able to use the authorization methods to protect their data as needed. For example, the data owners must control which users are allowed to view certain columns of data, provide column-wise data access authorization along with user group management.

Consent management framework/platform

By implementing an effective consent management platform, the following objectives can be achieved:

i. A standardized data collection management across all points where personal data is collected using consent as the lawful basis.

ii. Adequately align with regulatory requirements in turn lowering the risk of non-compliance with privacy regulations.

iii. The ability to monitor consent and withdrawal of consent in turn facilitating effective management of Data subject rights.

iv. The ability to interface with the respective data base where personal data was collected using consent and perform the necessary operations thereafter.

v. Effective governance across all related platforms so to have an overview of all the consents the organization has received.

Cookie preference management

i. Implementing cookie scanning technologies will help identify cookies that usually are not identified manually or unknowingly introduced by a third party.

ii. With more awareness on data privacy laws, more consumers are becoming concerned about their data privacy. By implementing a cookie preference management system, the following objectives can be achieved:

    a. Adequately align with regulatory requirements in turn lowering the risk of non-compliance with privacy regulations.

    b. Build confidence with customers by letting them choose what personal data is collected and how it is used.

    c. Help consumers to make informed choices effectively, in turn empowering consumers.

    d. Provide a platform for your marketing team to operate with a privacy-first approach and personalization in line with privacy laws.

Data classification and labeling

Implement a data classification and labeling tools ecosystem to facilitate effective data processing and protection ecosystem.

i. This will help an organization define a standard policy and categorize organizational data based on sensitivity and criticality, which then helps determine appropriate protection and retention controls on that data.

ii. Accordingly, data classification and labeling can automate label documents and artefacts via discovery/labeling engines and enable interface with the organizations DLP tool to ensure critical data is being monitored at the gateway of exit.

iii. Data classification and labeling also helps users to identify the sensitivity of data/documents/emails etc. and in turn build a more responsible user environment.

Data subject rights management

i. Implementing a DSR management platform/application enables an organization to manage DSR requests in one place and channelize fulfilment of DSR effectively.

This can facilitate a number of actions from receipt of a DSR request to its authentication and validation and in turn mapping the DSR to the respective stakeholder to enable the fulfillment of the DSR request.

ii. This may help an organization save time and resources. Managing a DSR via spreadsheet, phone log or email is relatively time consuming and tedious.

iii. A good DSR management system will help interface with relevant departments, and data discovery tools to enable an effective and seamless workflow.

iv. The architecture should ensure an API based model or micro services is implemented to interface with the subject rights management system and the respective data storage.

v. A DSR management platform/application provides holistic dashboards for effective governance.

Automated assessments

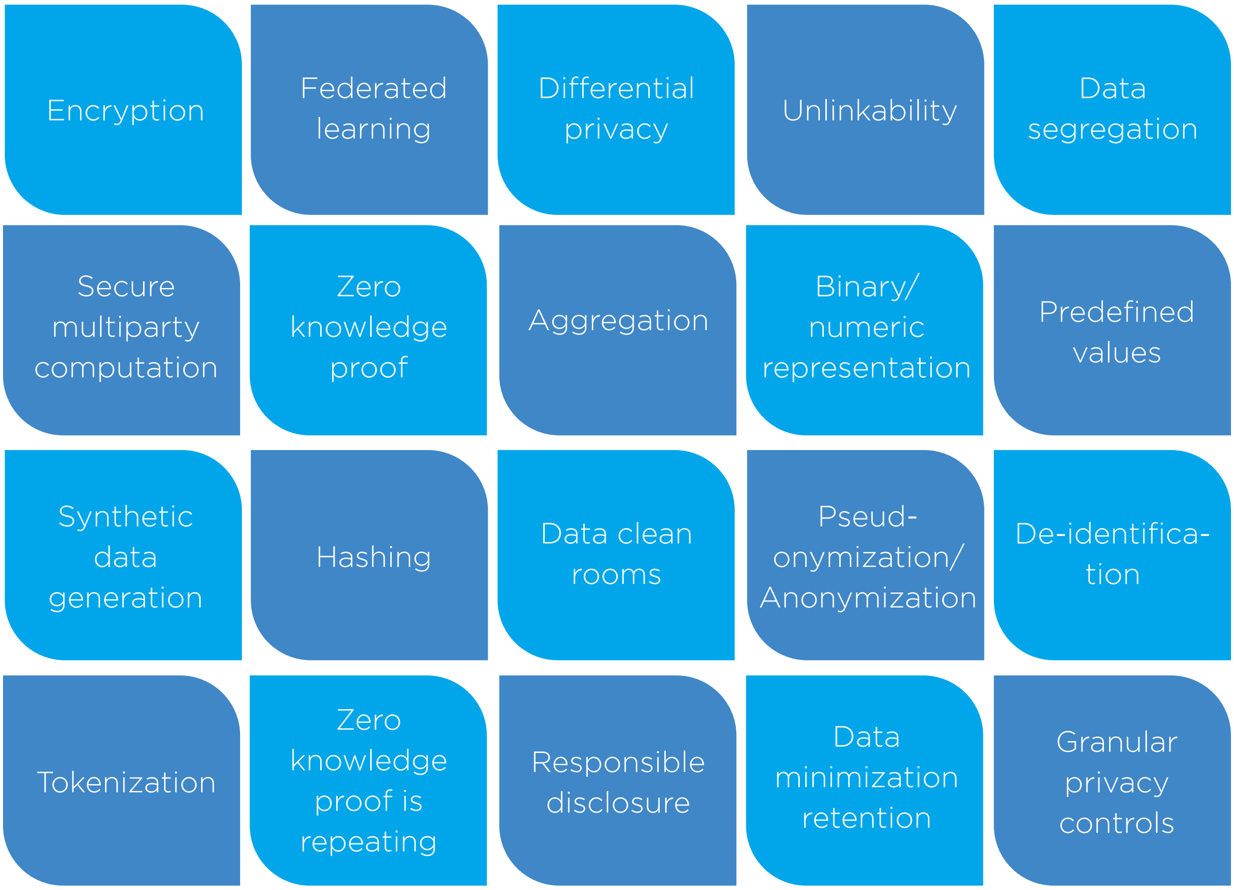
Incorporate an automated impact assessment procedure by adopting assessment tools so the applicable risks of processing personal data are automatically tagged and can be tracked to closure. Adopting such automation can also enable centralized dashboards and provide a single view of the risks of processing personal data.

This approach will also help the organization understand the activities it performs on the different kinds of data it collects and processes and effectively populate the data inventory and ROPA workflow.

Such workflows can also be extended to privacy audits so the entire life cycle of the data being processed can be captured and documented in one centralized repository.

7.3 Adoption of Privacy Enhancing Technologies

Privacy laws globally recommend and mandate organizations, both data controllers and data processors, to implement appropriate technical and organizational measures. This will ensure maintaining the confidentiality, integrity, availability of data and its processing systems and services and minimize accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed. Some of these measures have been explored in this sub-section below.



Encryption	Federated learning	Differential privacy	Unlinkability	Data segregation
Secure multiparty computation	Zero knowledge proof	Aggregation	Binary/ numeric representation	Predefined values
Synthetic data generation	Hashing	Data clean rooms	Pseud-onymization/ Anonymization	De-identifica-tion
Tokenization	Zero knowledge proof is repeating	Responsible disclosure	Data minimization retention	Granular privacy controls

Encryption

i. Encryption is implemented to secure data from being stolen, compromised, or altered. A basic encryption methodology/algorithm secures data into a secret code that can only be unlocked with a unique encryption key.

ii. Encrypted data can be protected while at rest or in transit, or at the time of being processed. This must be applicable irrespective of the location of the asset, be it on-premises or remote cloud servers.

iii. It is used for protecting personal data keeping in mind both integrity and confidentiality.

Encryption converts normal data to encoded information, that can be decoded with a unique decryption key. The different types of encryption techniques are briefly highlighted below.

a. **Symmetric or private key cryptosystems**: Using the same key for encryption and decryption.

b. **Asymmetric or public key cryptosystems**: Using different keys for encryption and decryption. A user uses two keys (public and private) which is executed via digital certificates.

c. **Hybrid cryptosystems** are also one of the options that can be used. Here, encryption is undertaken with a public key algorithm. The recipient decrypts with his/her private key.

d. **Homomorphic encryption** is a form of encryption that allows mathematical operations to be performed directly on the ciphertexts, producing an encrypted result that, when decrypted, matches the result of the same operations performed on the plaintexts.

   It allows you to do calculations on the encrypted data as if it were unencrypted, without having to decrypt it first. This has the potential to enable a wide range of applications, such as secure cloud computing and secure search over encrypted data.

   - Secure machine learning homomorphic encryption could be used to allow organizations to securely train machine learning models on sensitive data, while also protecting the confidentiality of the data.

   - Secure e-commerce homomorphic encryption could be used to allow organizations to securely process sensitive data in the context of e-commerce transactions, such as in the case of online payment processing or customer data management.

   - Secure data processing homomorphic encryption could be used to allow organizations to securely process sensitive data, while also protecting the confidentiality of the data, such as in the case of data analytics or machine learning

iv. Identify sensitive personal data and implement encryption of such data.

a. This can be done at a database level, data element level, or column level.

b. Both data at rest and data in transit must be encrypted based on the sensitivity and criticality of such data.

v. Use encryption methodologies that have secure key processing.

a. Triple DES (3DES or TDES), RSA, Twofish, The Advanced Encryption Standard (AES), Blowfish, Format Preserving Encryption (FPE), etc.

b. Symmetric and asymmetric encryption

vi. It is good practice to rotate and set a lifetime for an encryption key (for example, rotate every two months, set lifetime).

vii. Practice effective protection mechanisms. Adopt dual encryption for sensitive personal data.

viii. The encryption key must be stored in a safe place, preferably in a different environment that stores the sensitive information.

Federated learning

Federated learning is one of several emerging privacy-enhancing technologies steadily gaining traction with its capability to train algorithms on various data sets without exchanging raw data artificial intelligence applications, such as language translation, voice recognition and text prediction apps, typically require large-scale data sets to train high-performance machine learning models such as deep neural networks.

There can be challenges when the data needed to train the model is personal or proprietary. On the other hand, federated learning enables ML models to operate without moving the personal data needed for training to a central server. The raw data never leaves the device and is never collected in a central location. Instead, the ML model itself is sent to edge devices — mobile phones, laptops, Internet of Things devices or private servers — to be trained. Some applications include:

i. Next-word prediction and emoji suggestions.

ii. Use cases in autonomous vehicles fault detection, and IoT devices monitoring/ preventive maintenance.

Differential privacy

It refers to a mathematical technique of adding a controlled amount of randomness to a dataset to prevent anyone from obtaining information about individuals in the dataset. The added randomness is controlled. Therefore, the resulting dataset is still accurate enough to generate aggregate insights through data analysis while maintaining the privacy of individual participants. Some applications include:

i. Collecting telemetry data from apps/devices for application performance monitoring.

ii. Synthetic data generation.

Unlinkability

It refers to a scenario where data is being stored to establish a diverse storage mechanism that facilitates unlinkability. As a result, if a data set is exposed using such data will be difficult.

Data segregation

i. It is the process of separating data sets from one another so that different access policies can be applied. Organizations should implement partitions between datasets or types of data, to which different access and usage policies are applied.

ii. Such segregation can prevent data leakage or improper access. Segregation also facilitates in third party data sharing or internal processing when operations like analytics is being performed at an organizational level.

iii. Data segregation is a very effective way for storing personal data or any other data.

iv. This can be accomplished by physical or logical segregation/distributed across different tables/compartments.

v. A virtualized data layer can also be used. Data can be accessed inside an environment without transferring to a different location for processing.

Adopt aggregation

When representing sensitive personal data such as in analysis or reporting, adoption of aggregation values is ideal. This will avoid exposure of detailed data points. Typically, most of such data reporting will not need detailed reporting. Detailed reporting/access must be highly access controlled and must lie with function heads.

Adopt binary/numeric representation

A good practice to follow is binary representation of data. Binary representation of data will not expose the real data at the first stage of data storage. For example, when collecting diversity data use binary values on the user screen: 1-Male, 2-Female, 3-Others. The value that is stored in the primary record will be the binary value. To process this data point, another table holding this correlation will need to be used.

Use predefined lists

This can avoid collection of incorrect/inaccurate data or multiple versions of data. For example, choosing the name of a country from a list of countries rather than typing the name of a country in free form text.

Synthetic data generation

i. It refers to data that is artificially created. It is often created with the help of algorithms. Synthetic data is typically used for creating test data for products, applications and tools, validation purposes, and in AI model training. Synthetic data is a type of data augmentation.

ii. Use cases include:

  a. Fraud and anomaly detection in Telecom and Banking

  b. Training AI Models

iii. Using synthetic data is ideal for operations in the lower environments like test environments.

Secure Multi-Party Computation (SMPC)

Secure multi-party computation is an encryption methodology. It allows multiple parties to collaborate on encrypted data. Similarly, to homomorphic encryption, the goal here is to keep data private from participants in the computational process. Key management, distributed signatures, and fraud detection are some of the possible use cases here. The limitation of secure multi-party computation is the resource overhead. To pull off an SMPC stunt with success is pretty tricky - everything has to be timed right and processing has to happen synchronously.

Zero-Knowledge Proof (ZKP)

ZKP is a set of cryptographic algorithms that enable information to be validated without revealing data that proves it. It plays a crucial role in identity authentication. An individuals age, for example, can be authenticated with ZKP without disclosing their actual date of birth.

Adopting hashing algorithm

An organization can adopt a hashing algorithm (like SHA-256), for identifiers such as an email address or phone number which in turn produces a hashed identifier. This identifier can now be used for all purposes in turn not exposing the actual value of the data.

Explore usage of “data clean rooms”

Explore usage of data clean room to collaborate more to collaborate more effectively with minimum intrusion.

Anonymization/Pseudonymization

GDPR calls out **Pseudonymization** as “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information”. Anonymization/Pseudonymization are typically used to prevent linking data to the original identity of a person. As a result, limiting the consequence of data exposure. It changes the original data with an alias.

i. **Pseudonymization** means changing real data into unreal data. For ex: change the name John Smith to xovr tergih. This will help retain the characteristics of the original data but will not allow you to identify the original data with the algorithm used for Pseudonymization. Similarly, a phone number can be interpreted as 9898989898 (original) to 0100133022. This can be used when you are sharing data with third parties who need to process data for you but dont need to see personal identifiers of the data being processed.

ii. Anonymization can be done to de-identify data (especially during retention without being able to link). Anonymization can also be adopted when there is a need to create test data.

iii. **Data masking** - Hiding data with special characters/values.

iv. **Data perturbation** - Modify data applying numbers and random noise.

v. **Synthetic data** - Create fabricated data or artificial datasets from a model of the original data containing only properties and not real data.

Use techniques like de-identification using noise, masking etc.

i. The process of de-identification removes personally identifiable information. For example, this can be achieved by replacing existing data with characters or text variables.

ii. Erasure is a technique where certain data is eliminated, so that the person concerned is no longer identifiable.

iii. Generalization involves replacing information with a pointed value with a different value or a broader category value. For example, age can be replaced with age ranges.

Tokenization

Tokenization is about substituting real data like a national ID or a bank account number, with a substitute, known as a token. The token is randomized data that has no meaning. De-tokenization gives back the actual data element after the relevant token is provided.

Data minimization

i. Adopting data minimization techniques can directly reduce the amount of personal data that is being processed. With lesser data to process, the probability of data exposure also decreases.

ii. Data minimization techniques also ensure creation of multiple copies of the same data as a result reducing the footprint of such data. Encourage using already present data in the systems as majority of the time such data is used only for display or reporting purposes.

Data retention

i. One of the effective implementations of principles of processing is to establish a data retention policy to ensure data that is not needed by an organization anymore is deleted from the organizations repositories. Storing data indefinitely and without a defined purpose can cause significant storage and processing overhead that can impact an organizations analytics environmental impact.

ii. It is best to implement data retention timelines in an automated manner so the entire data trace can be factored in and ensured retention applies.

iii. Automate data retention via tools and OEM platforms. Tools such as a data lifecycle management enable deletion of records based on the retention schedule set. OEM platforms have built in add on modules to enable data retention/deletion.

iv. One such method is to implement data retention algorithms into systems at the time of development of applications.

v. Understand the data landscape and build API based models or micro services to implement a data retention workflow.

Granular privacy controls

i. The most effective way to control collection of personal data is to implement granular privacy controls. Adoption of such a practice will ensure aligning with privacy principles of collecting and processing in a transparent manner (lawfulness, fairness, and transparency). collecting only what you need (data minimization). using it only for a particular purpose (purpose limitation).

ii. Such controls will also help in deleting data that is a result of an opt out or falls under data retention timelines.

8 Building a Privacy Culture in an Organization

A key aspect for an organization to adopt an effective data privacy framework, is for the organization to have a very strong privacy culture. A strong privacy culture can be established if the organization chalks out the following clearly:

Data strategy

It is the foundation to an organizations data practices. A data strategy is a plan that defines how an organization will process the data it collects, stores, shares, and processes all through the data lifecycle. The strategy must explain how the organization will enable ethical processing using technology, processes, people, and what rules it adopts to be able to manage an organizations information/data/assets.

The data strategy of of an organization must be strongly supported by:

i. Its top management/executives

ii. Its data champions from the business

iii. Subject matter experts from departments or functions

iv. All personnel associated with data processing.

Data governance framework

Data governance is a measure of a companys control over its data. Organizations today collect and process significant amounts of data from various sources. Data governance helps organizations manage and help mitigate the risk of processing such data and provides guidance on how to maximize value.

Establishing a reliable data governance framework will enable an organization to know how data is collected, from which source, for what purposes, where the data is stored, and how it is being processed and used, in line with the applicable law and whether it is adequately protected.

The governance framework will also measure/ensure the data strategy of an organization is being percolated and adhered to by all stakeholders in the organization.

The data governance framework can be successful if:

i. Its people are well versed on effective and secure data processing and management.

ii. A set of policies and processes are defined and adhered to.

iii. The framework is equipped with relevant technology interventions.

An effective data governance framework builds controls helps organizations adhere to regulatory compliances seamlessly.

Data protection framework

A significant part of data strategy and data governance is to ensure the organization protects the data of its customers and data subjects/principals. As a result, it is very crucial that the organization must define its data protection framework that is governed as a part of the organizations data governance framework.

This framework must comprise of all the applicable controls the organization defines and incorporates to ensure the data is collected and processed in a secure manner. This framework will include a set of process controls and technical interventions/controls it puts together for secure data processing. This will ensure organizations data has the highest standards of integrity and is not being misused or mishandled.

To be able to establish a strong privacy culture, the key objective of a data privacy organization must be to play the role of a facilitator and not a compliance master. The privacy function must therefore work in collaboration with Business, Delivery, Security, and IT functions.

The data privacy function must be envisioned as a role to strengthen the process, make a product more compliant with privacy laws, enable better management of personal data in line with applicable laws, and help in avoiding regulatory non-compliances and legal implications.

Parallelly, this can result in an opportunity to achieve more customer/user trust and at the end of the day a competitive advantage.

Some examples can be:

i. HR/Employee data

a. Helping to process data lawfully in line with data minimization, appropriate consent management, sectoral nuances such as lawfully collecting diversity related data (where permitted by law) and ensuring right controls are adopted for data collection, sharing and usage.

b. Ensuring sectoral laws are taken into consideration and a holistic view of processing personal data is looked at.

ii. Marketing data

a. Helping adopt a cookie preference center.

b. Helping adoption of a centralized sales database rather than a local database to ensure accurate data is used and the importance of adopting a centralized consent withdrawal/DSR request management.

c. Sensitize on the importance of stronger contracts with vendors enabling the organization with prospective contacts for marketing activities.

iii. Application development

a. Enabling the team with the right technical guidance such as encryption, de-identification, aggregation, etc. An example may be the process of building an application that collects diversity related data, and interventions may be to implement data segregation, anonymization at source, report using aggregation with a strong role based access.

b. Provide checklists to ensure privacy norms are considered upfront in the design stage of building, onboarding any application.

iv. Vendor management

a. Ensuring adherence to the correct Data Processing Agreement (DPA) and emphasizing accountability are essential for the data processor and sub-processor.

b. Help assess the vendors data privacy posture, technical and organizational processes, as well as the incident management process, etc.

v. Information technology

a. Help adopt a structured decommissioning process, implement an automated data retention process considering both upstream and downstream applications, and establish data classification and labeling, etc.

b. Establish a practice to ensure the implementation of Privacy by Design (PbD) in applications being developed for the organization.

c. Provide comprehensive checklists and ensure their easy understanding to facilitate the implementation of Privacy by Design (PbD) practices.

vi. Security

Facilitate increased awareness of employee monitoring laws and regulations to ensure the lawful processing of data, etc

vii. Delivery/Customer services

a. Sensitize the team on the importance of the obligations of a data processing agreement.

b. Increase awareness of the need for not accepting controllership without proper risk assessment.

c. Evaluate the liability aspects thrown at you for processing personal data of customer/end customer.

d. Sensitize teams to ensure usage of non-production data in non-production environments.

e. Create awareness to implement PbD into applications being developed for the customer.

Encouraging privacy champions, training, and onboarding business specific personnel to help the privacy team facilitate the adoption of data privacy practices across the organization. To incorporate privacy in the cultural ethos of the organization, impact assessment exercises should be facilitated rather than asking business functions to independently implement privacy.

The privacy team must continuously explore opportunities to interface and liaison with other functions to communication, create awareness and sensitize different departments and business functions about the importance of adhering to data privacy laws. This can be done though periodic sessions, incident-based sessions, role-based sessions, quizzes, awareness on usage of new technologies, etc.

Finally, updating senior management on the adoption of these practices and the benefit the organization is achieving from doing so in turn becomes a differentiator and creates competitive advantage. Achieving adequate managerial support is necessary to be able to achieve the goals set and be compliant with privacy laws.

9 Conclusion

While use of personal data is fundamental to the development and growth of a variety of businesses and services, introducing checks and balances is a necessity to ensure the potential of harm to individuals and their rights is minimized – not as an after-thought but by design.

Privacy by Design provides a framework for a holistic approach that can be adopted by an organization in protecting the privacy of their stakeholders across the spectrum, including their customers and employees among other parties. Adopting Privacy by Design is proven to have a direct positive impact on the reputation, trust and value of an organization while also holding the potential to reduce regulatory actions, if operationalized and implemented satisfactorily.

This needs to be accompanied by a change in mindset and culture, as well as a commitment to follow the principles and practices that ensure privacy is embedded in every stage of the product or service lifecycle. While this is not a one-size-fits-all solution, it presents itself as a highly adaptable and flexible framework that can be tailored to the specific context and objectives of each organization.

Future versions of this working paper developed using the principles highlighted herein as a foundation may entail illustrative guidance for specific case studies. For instance, application of privacy by design principles to processing undertaken for marketing purposes or to processing of employees personal data could provide valuable insight into the manner in which these principles and ideas can be translated into organizational practices.

10 References and Additional Reading Material

- AEPD, A guide to Privacy by Design, https://www.aepd.es/es/documento/guia-privacidad-desde-diseno_en.pdf
- IAPP, Spanish DPA Guidance on AI-based data processing, https://iapp.org/resources/article/spanish-dpa-issues-guide-on-ai-based-data-processing-2/
- Ann Cavoukian, The 7 Foundational Principles, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
- Personal Data Protection Commission, Basic Anonymisation, https://www.pdpc.gov.sg/Help-and-Resources/2018/01/Basic-Anonymisation
- Ann Cavoukian, Operationalizing Privacy by Design, https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf
- Anna Romanau, The necessity of the implementation of Privacy by Design, https://www.sciencedirect.com/science/article/abs/pii/S0267364917302054?via%3Dihub
- EDPB Guidelines on Article 25, Data Protection by Design and Default, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf
- Article 29 Working Party Opinion on Anonymisation Techniques, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
- U.K. ICO, Direct Marketing guidance, https://ico.org.uk/media/1555/direct-marketing-guidance.pdf
- U.K., Direct Marketing Checklist, https://ico.org.uk/media/for-organizations/documents/1551/direct-marketing-checklist.pdf
- Statista, Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025,

https://www.statista.com/statistics/871513/worldwide-data-created/#:~:text=The%20total%20amount%20of%20data,replicated%20reached%20a%20new%20high

- OneTrust, Steps to comply with ISO 31700 standard on Privacy by Design, https://www.onetrust.com/blog/7-steps-to-comply-with-iso-31700-12023-standard-on-privacy-by-design/
- ClearCode, Privacy Enhancing Technologies, https://clearcode.cc/blog/privacy-enhancing-technologies-pet/
- ClearCode, Data Clean Rooms interview, https://clearcode.cc/blog/data-clean-rooms-interview-aqilliz/#data-clean-rooms-for-ad-targeting-audience-targeting-measurment
- Skyflow : Keep Sensitive Data Out of Your Logs: 9 Best Practices https://www.skyflow.com/post/how-to-keep-sensitive-data-out-of-your-logs-nine-best-practices
- OWASP : Session Management Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html
- Designers : The Danger of Dark Patterns https://www.toptal.com/designers/ux/dark-patterns
- AI Multiple : Top 10 Privacy Enhancing Technologies & Use Cases in 2023 https://research.aimultiple.com/privacy-enhancing-technologies/
- Mostly AI : What are privacy enhancing technologies? The 5 best PETs for the modern tech stack https://mostly.ai/blog/what-are-privacy-enhancing-technologies
- TechTarget : Privacy-enhancing technology types and use cases https://www.techtarget.com/searchsecurity/tip/Privacy-enhancing-technology-types-and-use-cases
- U.K. ICO, What types of encryption are there?, https://ico.org.uk/for-organizations/uk-gdpr-guidance-and-resources/security/encryption/what-types-of-encryption-are-there/#:~:text=There%20are%20two%20types%20of,used%20for%20encryption%20and%20decryption.
- Cloudian, Data Encryption: The Ultimate Guide, https://cloudian.com/guides/data-protection/data-encryption-the-ultimate-guide/
- SimpliLearn, What Is Data Encryption: Types, Algorithms, Techniques and Methods, https://www.simplilearn.com/data-encryption-methods-article

- Google Cloud, What is encryption?, https://cloud.google.com/learn/what-is-encryption

- Imperva, Anonymization, https://www.imperva.com/learn/data-security/anonymization/

- U.K. ICO, Anonymisation Guidance, https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf

- AIMultiple, Top 8 Data Masking Techniques: Best Practices & Use Cases, https://research.aimultiple.com/data-masking/

- Johns Hopkins Sheridan Libraries, Protecting Human Subject Identifiers, https://guides.library.jhu.edu/protecting_identifiers/de-id_steps

- Bisok, 5 facts about data de-identification and the best methods, https://blog.bisok.com/general-technology/5-things-you-need-to-know-about-data-de-identification-and-why-its-so-important

- Immuta, What is data redaction?, https://www.immuta.com/blog/what-is-data-redaction/

- Imperva, Tokenisation, https://www.imperva.com/learn/data-security/tokenization/

- AWS security blog, How to use tokenization to improve data security and reduce audit scope, https://aws.amazon.com/blogs/security/how-to-use-tokenization-to-improve-data-security-and-reduce-audit-scope/

Authors

Jagannath PV
Global Data Privacy Officer
LTIMindtree
https://www.linkedin.com/in/jagannath-pv-a6875b5/

Aswathy Asok
Vice President (Global Data Privacy and Retention)
HSBC
https://www.linkedin.com/in/aswathy-asok/

Dwarka Srinath
Chief Digital Information Officer, Tata Power
https://www.linkedin.com/in/dwarka-srinath-88b05b14/

Vindhya Vishwanath Kudva
Regional Data Protection and Information Security Officer
Bosch India

Contributor

Shivangi Malhotra
Associate- Privacy and Policy, DSCI
https://www.linkedin.com/in/shivangi-m/

NOTES

DSCI

PRIVACY
LEADERSHIP FORUM