

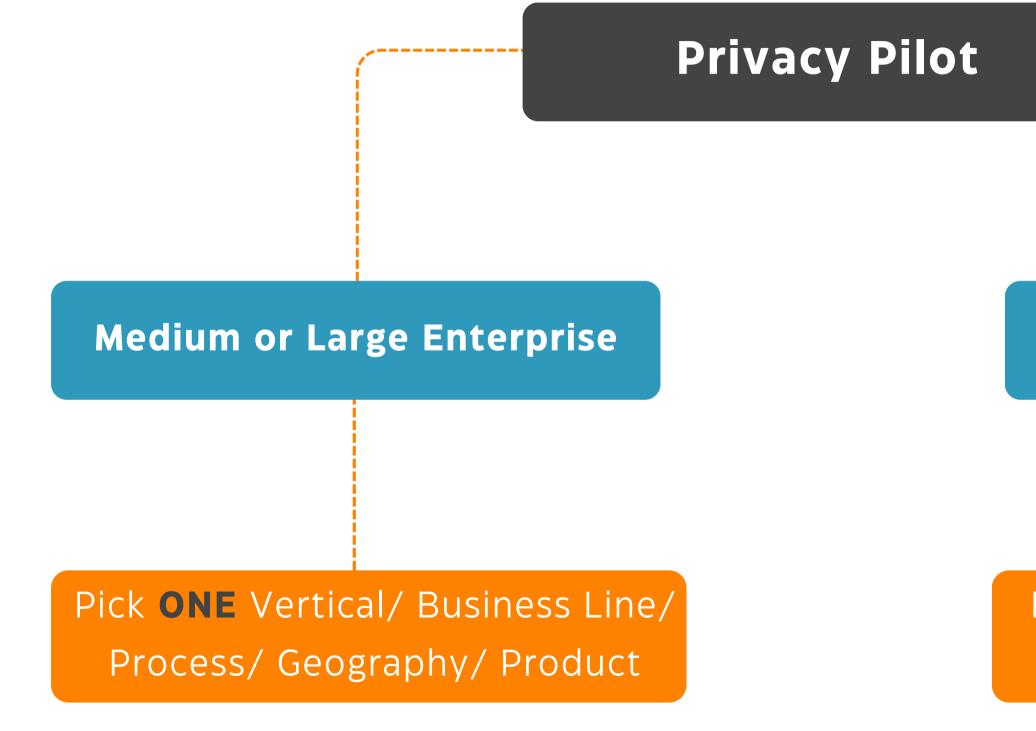
IMPLEMENTING COMPLIANCE TO THE DPDPA

A READY RECKONER

privacy@arrka.com | www.arrka.com



FIRSTLY, START SMALL

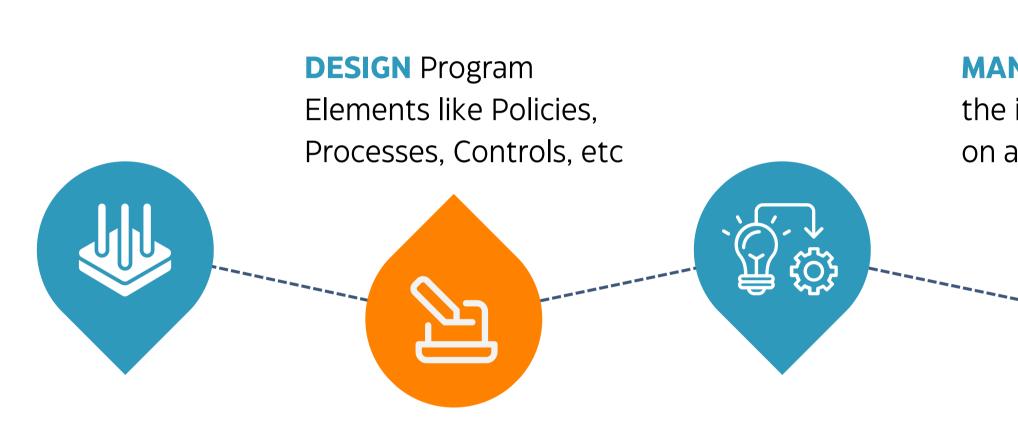


Make this the **Scope** of your Privacy Pilot



Pick your core business related aspects

ADOPT THE FOLLOWING APPROACH FOR THE PILOT



FOUNDATION

Understand Key Attributes of Organizational Personal Data/ Understand Existing Security Profile.

IMPLEMENT the

Program Elements across the Vertical/ Business Line/ Process/ Geography/ Product in scope

MANAGE & SUSTAIN the implementation on an ongoing basis

TRAINING & AWARENESS

for various target groups as required

STEP 1: LAY THE FOUNDATION



1. What Personal Data (PD)* is being processed

2. What are the channels of collection?

3. Where & how is your PD stored

1) Provided by the user

• Via paper-based forms** • Via your Website/ Mobile Apps

2) Observed by your Organization about the user

• Physically – via cctv cameras, sensors, etc Online – via cookies/ trackers/ App permissions/ etc

3) Generated by your Organization

• Eg: Usage Statements, Records, Logs, etc

4) Derived/ Analysed

• Eg: As a result of

Analytics

5) From Clients/ 3rd Parties

• Eg: If you are a Service Provider/ Processor, your client may provide you with Personal Data

• Eg: Your marketing dept may be procuring a leads database from a 3rd party

*Remember, Data Privacy focuses ONLY on Personal Data. However, what constitutes Personal Data is more than what you may intuitively think it is. Look up the Primer on DPDPA to understand what falls under Personal Data

** While only Digital Personal Data is within the scope of this Law, capture this as you may be scanning/otherwise digitizing this data later in your business processes

5. What is each PD being used for

4. How is your PD Flowing?

• Retention Period

Applications

• Locations

By Various Teams

- Across Applications
- Across geographical boundaries
- To & from 3rd parties

NOW YOUR FOUNDATION IS READY.

USING THE INFORMATION FROM THE PDAM,

MOVE TO THE NEXT STAGE: DESIGN



STEP 2: DESIGN

DESIGN THE VARIOUS ELEMENTS OF YOUR PRIVACY PROGRAM

Design the Internal **Privacy Policy** (to guide the Organization)

Design the Privacy Notice for your Website/ App/ Other points of Collection



Design Data Principal Rights Request &

Grievance Redressal Processes

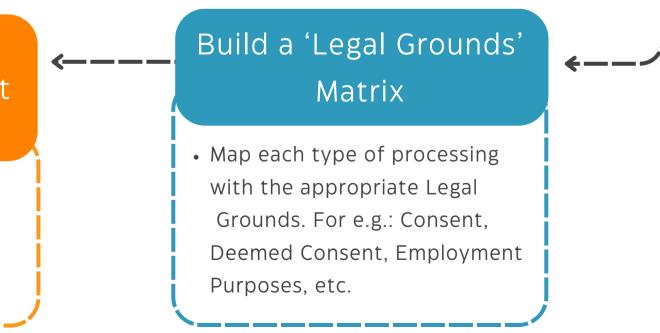
- Design Front End
- Set up Backend Process like Verification and Policies
- Ensure PD element mapping to various Rights

Design Consent Lifecycle Management Process

- Design Consent Text
- Build Linkages to downstream processes
- Ensure Audit Trails

Establish a Privacy Organization

• If yours is a small set up, identify who will 'own and manage' privacy in your current set up • If yours is a large organization, set up a formal DPO team, appoint Privacy Champions



Populate the Design Elements using Data from the Foundation Stage Use Existing Processes wherever possible and align Privacy Requirements to minimize disruption

STEP 2: DESIGN

Design the Various Elements of your Privacy Program

Set up a Third Party

Management Process

- Perform Privacy Due diligence
- Perform PDAM for each Third Party
- Update Contracts
- Establish stricter controls for high-risk Third Parties

Design various Privacy-Specific Processes

These include:

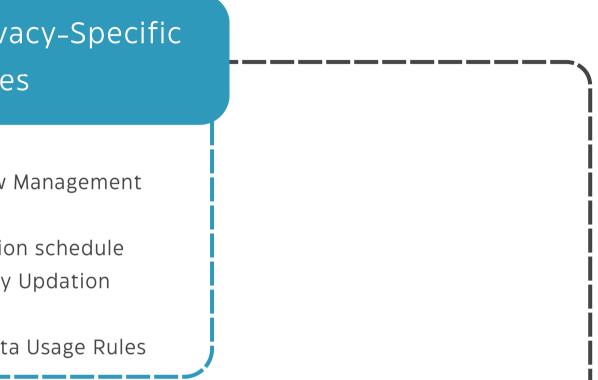
- Cross Border Data Flow Management
 Process
- Data retention & deletion schedule
- Personal Data Inventory Updation Mechanism
- Data Collection and Data Usage Rules

Monitor your Privacy

- Program
- Define Data Protection Impact
 Assessment Process to identify Privacy
 impact of changes
- Privacy KPIs
- Management Reviews
- Internal Audits
- Appoint External Auditor (if SDF*)
- External Audits

Organize Privacy Training

- Basic training for all users in the organization
- Specialist training(s) as required – for key people setting up and managing the program



Align your Security Program to address requirements of DPDPA

 In particular, update your security incidents management process to handle breach reporting

STEP 3: IMPLEMENT EACH DESIGN ELEMENT

Use an **AGILE** Approach :



For Example:



Implementation would involve

- Training the teams
- Handover of the Process
- Workflows (if any)
- Website/App changes

Roll Out

Roll out the process leveraging existing teams & applications. Set up a dedicated team if volumes are anticipated to be high

IMPORTANT

Each Design Element is intricately linked to multiple other design elements

For Example:

Request for Data Erasure

Authentication – part of **Security Program**

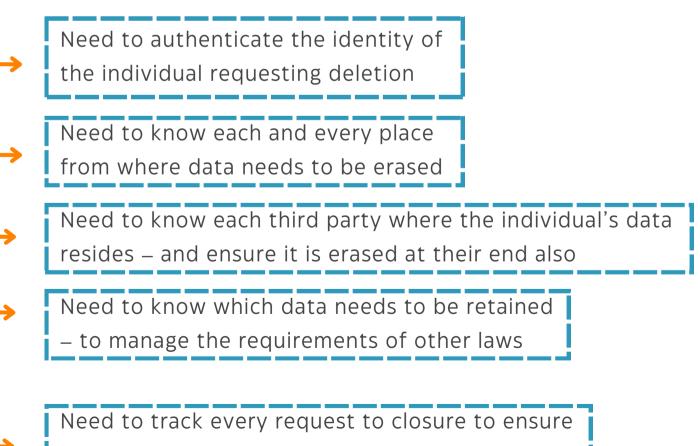
Personal Data Inventory

Third Party Management

Retention Schedule

KPIs and Metrics

It is important to determine those linkages and build them



DPDPA prescribed timelines are adhered to

ABOUT ARRKA

Arrka equips organizations to get compliant and remain compliant with any privacy law(s). Powered by the Arrka Privacy Management Platform, the Arrka Lab, Arrka Privacy Implementation Frameworks and Arrkademy coupled with over a decade of experience helping organizations set up and manage their privacy compliance journeys, Arrka makes Data Privacy simple, efficient and doable.

To make the DPDPA a reality in your organization, do get in touch with us at: privacy@arrka.com

Note: The approach and recommendations in this document are high-level, broad and non-specific, derived from Arrka's detailed implementation frameworks. Every organisation needs to adapt the same to it's context. This is not to be construed as legal and/or technical advice. Arrka is not a law firm