



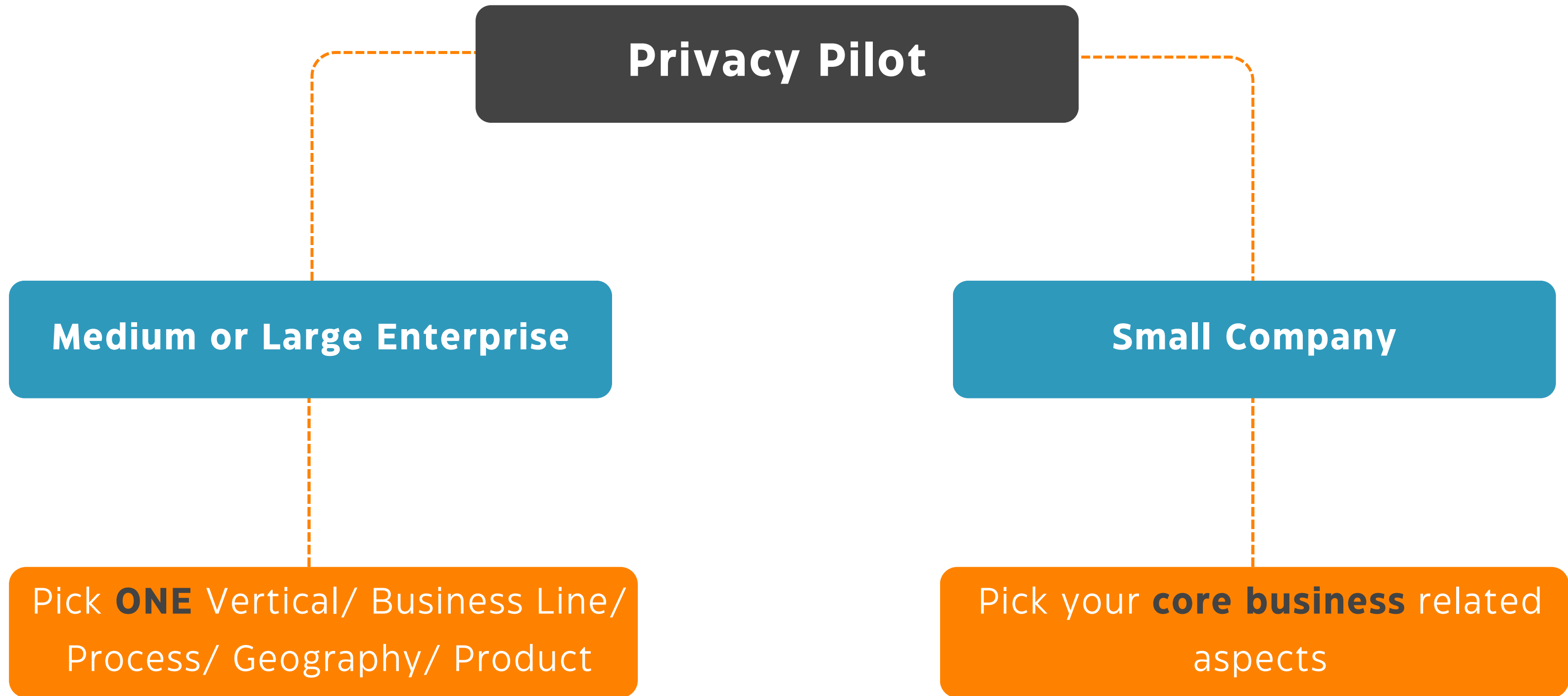
IMPLEMENTING COMPLIANCE TO THE DPDPA

A READY RECKONER

privacy@arrka.com | www.arrka.com

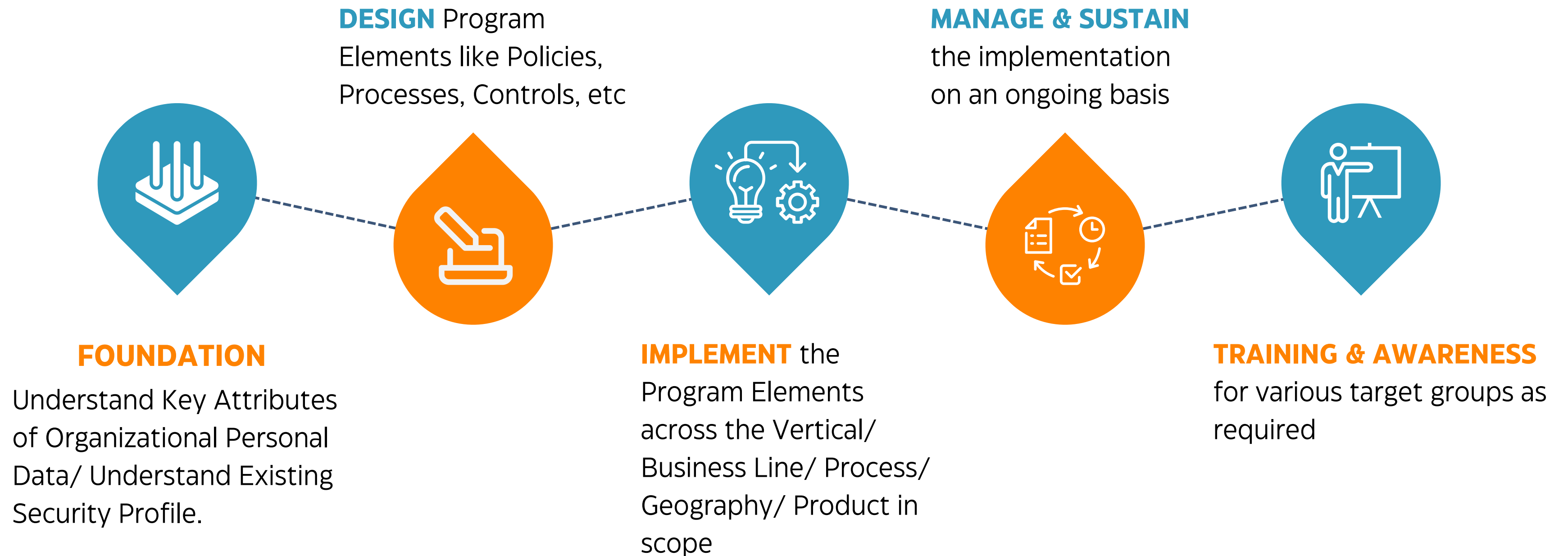


FIRSTLY, START SMALL



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

ADOPT THE FOLLOWING APPROACH FOR THE PILOT



STEP 1: LAY THE FOUNDATION

BUILD A **PERSONAL DATA ATTRIBUTE MAP (PDAM)**

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

2. What are the channels of collection?

3. Where & how is your PD stored

4. How is your PD Flowing?

5. What is each PD being used for

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

- Applications
- Locations
- Retention Period

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

By Various Teams

*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

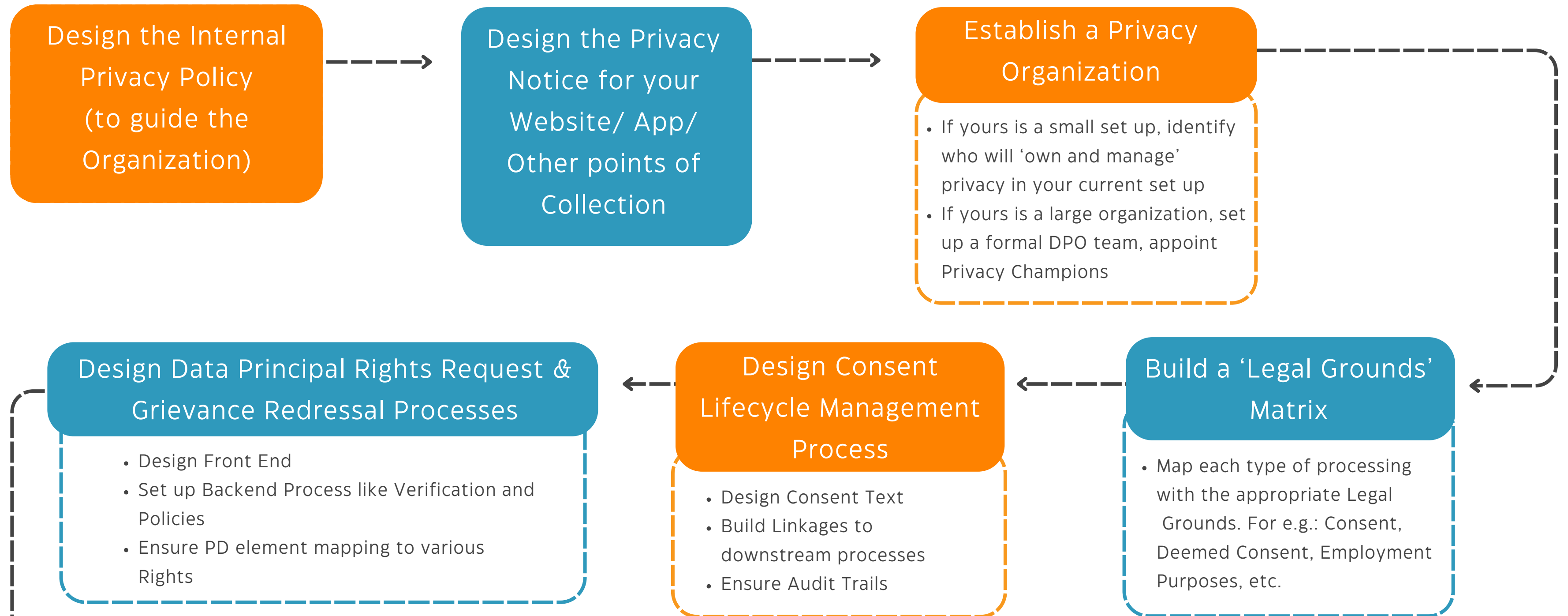
NOW YOUR FOUNDATION IS READY.

USING THE INFORMATION FROM THE PDAM,

MOVE TO THE NEXT STAGE: DESIGN

STEP 2: DESIGN

DESIGN THE **VARIOUS ELEMENTS OF YOUR PRIVACY PROGRAM**



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

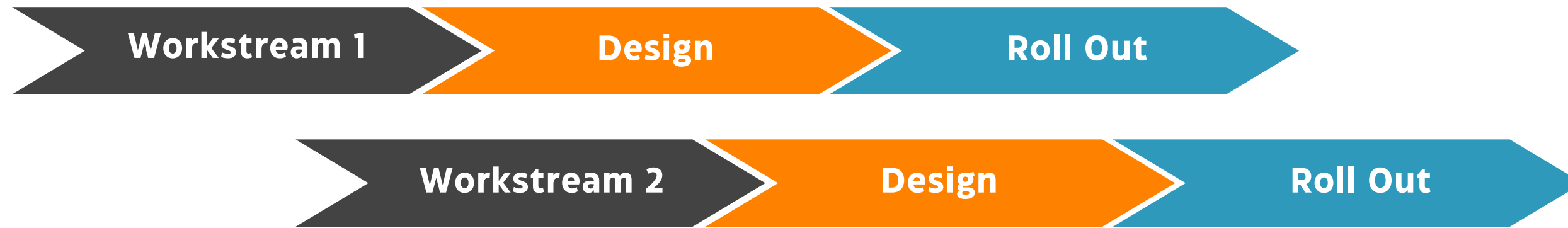
- Basic training for all users in the organization
- Specialist training(s) – as required – for key people setting up and managing the program

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

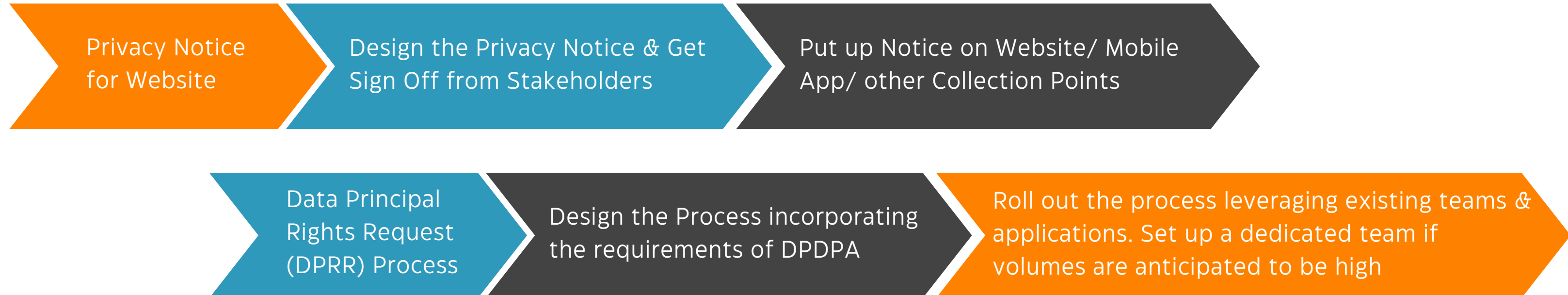
Use an **AGILE** Approach :



Implementation would involve

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

For Example:

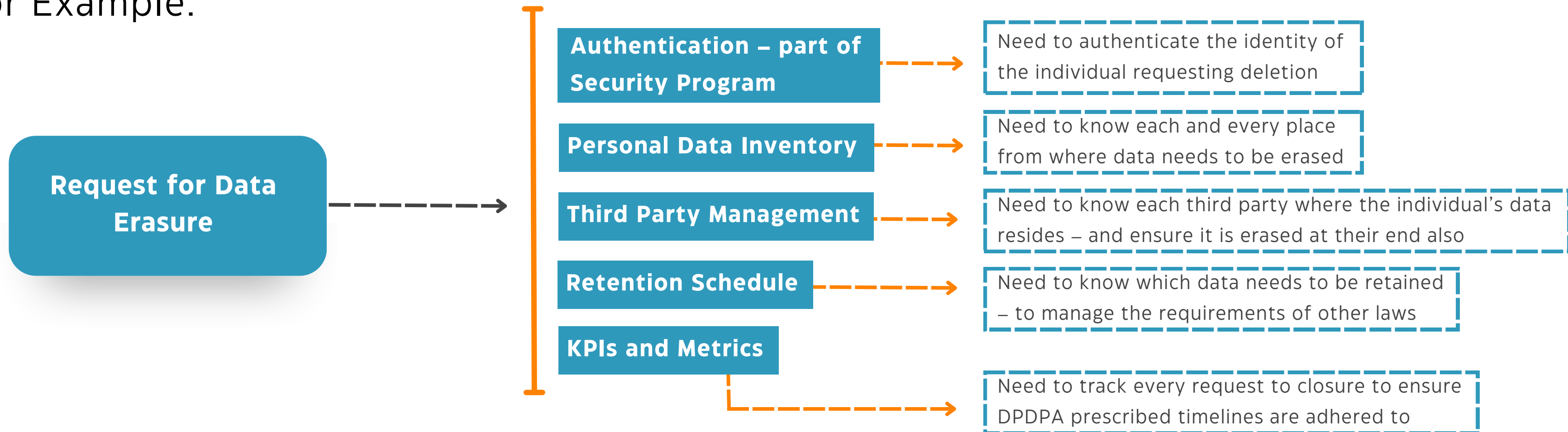


IMPORTANT

Each Design Element is intricately linked to multiple other design elements

It is important to determine those linkages and build them

For Example:



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 its context. This is not to be construed as legal and/or technical advice. Arrka is not a law firm