



– Innovate • Integrate • Transform –



SANJAY KAUSHAL

**Global Chief Information
Security Officer (CISO)**

Orbit Techsol India Pvt. Ltd.

23+ Years Cybersecurity Leadership

Member, **Data Protection Legislative Council**

Certified DPO

<https://www.linkedin.com/in/sanjay-kaushal-064ba312/>

Profile

Sanjay Kaushal is an action-oriented cybersecurity and technology leader with 25+ years of experience across cyber consulting, presales, solution design, delivery, and Security Operations Center (SOC) functions — leading large, complex transformation programs for marquee clients across India and global markets.

A results-driven strategic leader with deep expertise in cybersecurity, technology risk, enterprise risk, digital transformation, and emerging technologies, he is a trusted advisor to boards, CXOs, CIOs, and CISOs — aligning security and technology strategy with business objectives and risk priorities.

He builds and manages strategic relationships with clients, technology partners, media, and internal stakeholders, and leads Virtual CISO (vCISO) and cybersecurity advisory services that strengthen security posture and cyber resilience.

Certifications & Credentials

CISSP	CISM	CISA	CRISC	CIPM
CCISO	ISO 27K	CEH	ITIL	CCSE
MCSE	FSCA	JNCIS	FCNSP	CCNP
RCP	MCDBA	AWSCCS	PCNSE	



DATA PROTECTION LEGISLATIVE COUNCIL

Sanjay Kaushal
Global Chief Information Security Officer, Orbit Techsol India Pvt Ltd



Digital Personal Data Protection Act, 2023

Law and obligations of Government organisations

Includes DPDP Rules, 2025 (phased commencement)

The law at a glance

Who is covered

Any person or State body deciding the purpose and means of processing digital personal data: the Data Fiduciary. Government departments, PSUs and agencies are included.

What is protected

Personal data in digital form, or digitised later, processed in India (and some processing outside India for offering goods or services in India).

Core idea

Lawful processing for a specified purpose, with notice and consent, or a defined "legitimate use". Individuals (Data Principals) get enforceable rights.

Regulator

Data Protection Board of India: adjudicates breaches, directs remedial action and imposes penalties.

Lawful grounds for Government processing

Government bodies can rely on consent, but the Act also allows "legitimate uses" that suit public functions (Section 7):

- Subsidies, benefits, services, licences, certificates and permits, where the person has previously consented or the data is already in State records
- Performing a function under any law, or in the interest of sovereignty, integrity or security of India
- Compliance with a judgment, decree or order, or a legal obligation to disclose information to the State
- Medical emergencies, epidemics, disasters and public order situations
- Employment-related purposes (for staff data)

Even under legitimate use, the processing must stay within the purpose for which the data was collected.

Key obligations of a Government Data Fiduciary

Notice (S.5)

Tell people what data is collected, why, how to exercise rights and complain to the Board.

Accuracy (S.8)

Keep data complete and accurate where it is used to decide about a person or shared with others.

Breach reporting (S.8)

Inform the Board and affected persons of any personal data breach.

Grievance redressal (S.8)

Publish contact details of an officer or DPO and respond within the prescribed time.

Consent (S.6)

Free, specific, informed, unambiguous, with easy withdrawal, where consent is the ground.

Security (S.8)

Reasonable safeguards: encryption, access control, logging, monitoring and backups.

Retention (S.8)

Erase data once its purpose is served, unless law requires retention.

Children (S.9)

Verifiable parental consent; no tracking or targeted ads. Rules give exemptions for specified State uses.

Exemptions and special position of the State

What the State may be exempted from

- Section 17(2)(a): Central Government can notify State instrumentalities exempt from the Act, in the interest of sovereignty, security, foreign relations or public order
- Section 17(4): no duty to erase data once purpose ends (S.8(7)) and no right of erasure (S.12(3)) for State processing
- Research, archiving and statistical use meeting prescribed standards

What still applies

- Reasonable security safeguards and breach notification (unless specifically exempted)
- Purpose limitation and lawful ground for processing
- Rights of access, correction and grievance redressal
- State processing standards set under the Rules (Second Schedule)
- Exemptions must be notified and are open to judicial scrutiny

Why It Matters to Every Organisation

If you collect, store, or process the personal data of individuals in India — this law applies to you.

₹250 Cr

Maximum penalty per instance of non-compliance

All Sectors

Applies to govt., private, and non-profit data fiduciaries

Global Reach

Covers processing outside India tied to offering goods/services to Indians

No Cap

On the number of penalty instances the Board may impose

Non-compliance carries direct financial exposure, regulatory scrutiny, and reputational risk — making early readiness a business priority, not just a legal one.

Penalties for Non-Compliance

Financial penalties scale with the severity and nature of the failure — with no upper cap on total instances.

Failure to prevent a data breach	Up to ₹250 Cr
Failure in breach notification duties	Up to ₹200 Cr
Non-fulfilment of obligations for children's data	Up to ₹200 Cr
Non-fulfilment of additional obligations of Significant Data Fiduciaries	Up to ₹150 Cr
Breach of other duties by Data Principal	Up to ₹10,000
Breach of any other provision of the Act	Up to ₹50 Cr

Beyond the Fine

Penalties are levied per instance — repeated or systemic failures compound quickly across business units and data flows.

Proactive readiness — not last-minute fixes — is the only reliable way to keep exposure low.

Compliance roadmap for a Government organisation

1

Map data

Inventory personal data, systems, vendors and flows

2

Set lawful basis

Document the legal ground for each service and purpose

3

Notices and consent

Publish clear, bilingual notices; build consent where needed

4

Secure and log

Encryption, access control, log retention, vendor contracts

5

Breach playbook

72-hour detailed report process to the Board and individuals

6

Grievance and DPO

Name an officer, publish contacts, track rights requests

Most obligations take effect in phases under the DPDP Rules, 2025; confirm current dates in the Gazette.

Rights of the Data Principal

Every individual whose data is processed is entitled to the following:

1

Right to Access

Obtain a summary of personal data being processed and the processing activities.

2

Right to Correction & Erasure

Request correction, completion, updating, or erasure of personal data.

3

Right to Grievance Redressal

Readily available means to raise grievances with the fiduciary or Consent Manager.

4

Right to Nominate

Nominate another person to exercise these rights in the event of death or incapacity.

5

Right to Withdraw Consent

Withdraw previously given consent as easily as it was granted.

How Orbit Helps You Get Compliant

A structured, phased approach — aligned to Orbit's philosophy: Innovate · Integrate · Transform.

1

Assess

Data mapping & gap assessment against DPDP requirements across systems and vendors.

2

Design

Consent architecture, privacy notices, retention & breach-response policies.

3

Integrate

Technical controls — consent management, access governance, encryption, DPO workflows.

4

Sustain

Ongoing monitoring, training, audits, and Board-readiness support.

Orbit combines regulatory expertise with hands-on technical implementation — so compliance becomes part of how you build, not an afterthought.

How Orbit Helps You Get Compliant

A structured, phased approach — aligned to Orbit's philosophy: Innovate · Integrate · Transform.

1

Legal Consultancy

Data mapping & gap assessment against DPDP requirements across systems and vendors.

2

DPDP Tool

Consent architecture, privacy notices, retention & breach-response policies.
Implementation and migration

3

DPDP Operation

Technical controls — consent management, access governance, encryption, DPO workflows. Manage DPDP Operation

4

370 Security Professional

Across India 370 Security Professional

Orbit combines regulatory expertise with hands-on technical implementation — so compliance becomes part of how you build, not an afterthought.

The 8 Pillars of DPDPA 2023 Compliance



A Comprehensive Implementation Framework for Data Fiduciaries



Build Privacy into Culture



Govern Responsibly



Protect Personal Data



Enable a Trusted Digital India

01 Data Inventory & Processing Register

- ✓ Maintain records of personal data
- ✓ Document purpose, categories and flow of data
- ✓ Ensure accuracy & regular updates
- ✓ Map internal and external systems
- ✓ Identify data owners and responsibilities



02 Data Mapping & Data Flow

- ✓ Map data across functions, systems and locations
- ✓ Understand data flow within and outside India
- ✓ Identify storage locations and cross-border transfers
- ✓ Visualise data flow and dependencies



03 Consent & Legitimate Uses

- ✓ Obtain free, specific, informed and unambiguous consent
- ✓ Manage consent lifecycle (withdrawal, update, renewal)
- ✓ Ensure processing under lawful bases as per DPDPA
- ✓ Provide clear and simple notices



04 Data Principal Rights Management

- ✓ Enable access, correction, erasure & grievance redressal
- ✓ Provide easy-to-use channels for requests
- ✓ Respond within prescribed timelines
- ✓ Respect children's data protection requirements
- ✓ Maintain audit trail of requests



05 Privacy by Design & Security Safeguards

- ✓ Embed privacy in systems, products and processes
- ✓ Implement technical & organizational controls
- ✓ Follow data minimisation and purpose limitation
- ✓ Apply strong security measures (e.g., encryption, access controls, monitoring)



06 Personal Data Breach Management

- ✓ Detect, contain and assess breach incidents
- ✓ Notify the Data Protection Board & affected individuals
- ✓ Maintain breach register
- ✓ Take remedial action and prevent recurrence
- ✓ Conduct post-incident review



07 Vendor & Data Processor Governance

- ✓ Engage only compliant processors
- ✓ Ensure contracts with DPDPA-aligned clauses
- ✓ Monitor performance and conduct due diligence
- ✓ Audit processor practices
- ✓ Ensure data is handled as per agreed terms



08 Compliance Monitoring, Audit & Documentation

- ✓ Establish privacy governance structure and accountability
- ✓ Conduct regular audits and reviews
- ✓ Maintain evidence of compliance
- ✓ Track regulatory updates
- ✓ Drive continuous improvement



Accountability is the Foundation.

DPDPA promotes trust, transparency and responsible data practices for a safer digital ecosystem.

Why Every Organisation Needs DPDPA Compliance



Builds Customer Trust
Strengthens brand credibility and loyalty



Ensures Legal Compliance
Meets regulatory requirements



Reduces Regulatory Risk
Minimises penalties and reputational damage



Improves Data Governance
Strengthens processes and data quality



Enhances Privacy & Security
Protects personal data and sensitive information



Supports Business Growth
Enables responsible data-driven innovation



Contributes to a Stronger Digital India
Builds a trusted and inclusive digital ecosystem

DPDPA Compliance Roadmap – Key Steps



Assess
Understand current state and gaps



Plan
Define strategy, policies and ownership



Implement
Deploy controls and build capabilities



Monitor
Track compliance through audits and metrics



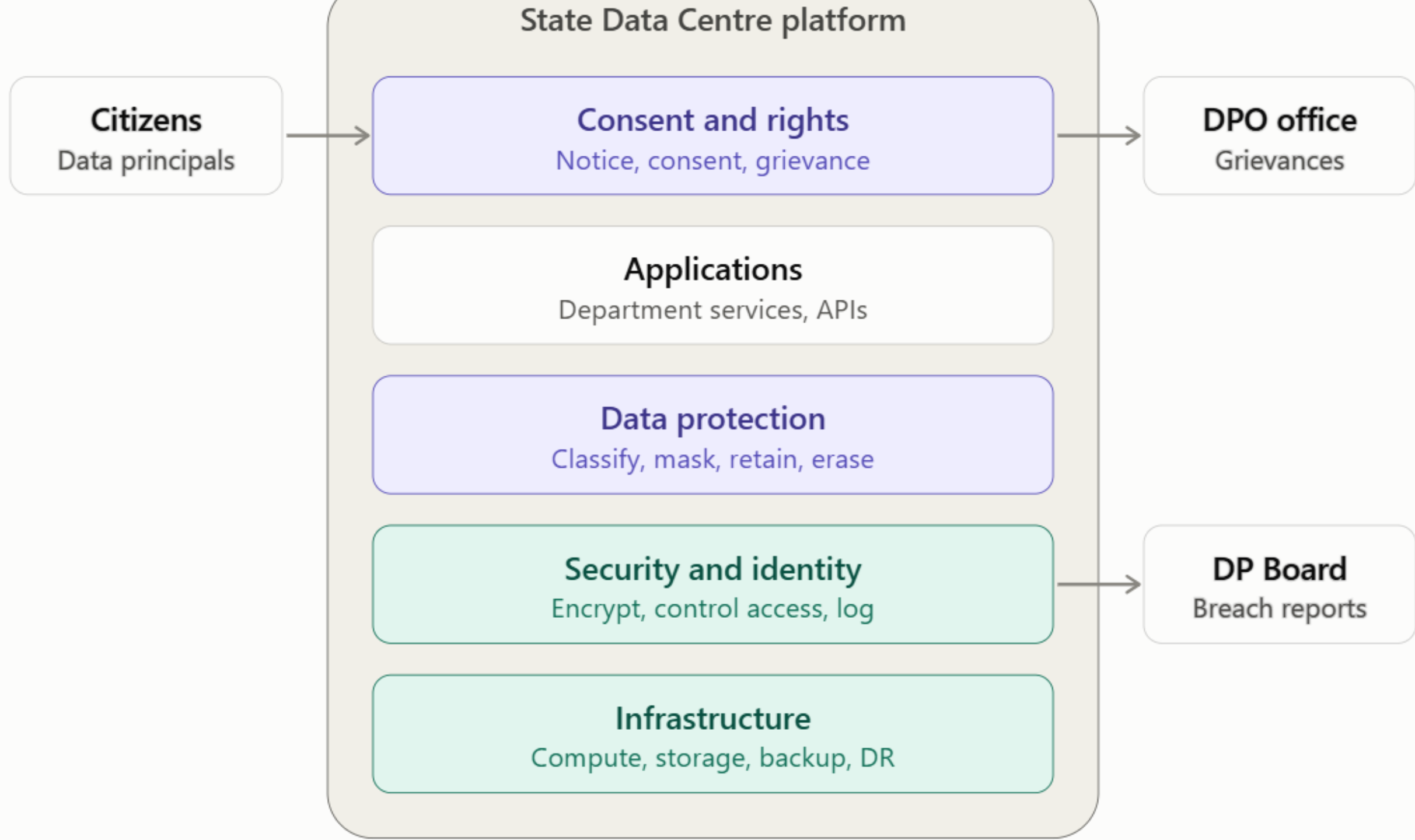
Improve
Evolve with regulatory changes and business needs

Additional Best Practices

- ✓ Maintain processing register
- ✓ Train & sensitise employees
- ✓ Conduct privacy impact assessments (PIAs)
- ✓ Review & assess third-party risks
- ✓ Implement retention schedule
- ✓ Test & improve incident response
- ✓ Review consent records periodically
- ✓ Keep policies documented and updated
- ✓ Foster a privacy-first culture
- ✓ Leverage technology for better compliance

Data Security Posture Management



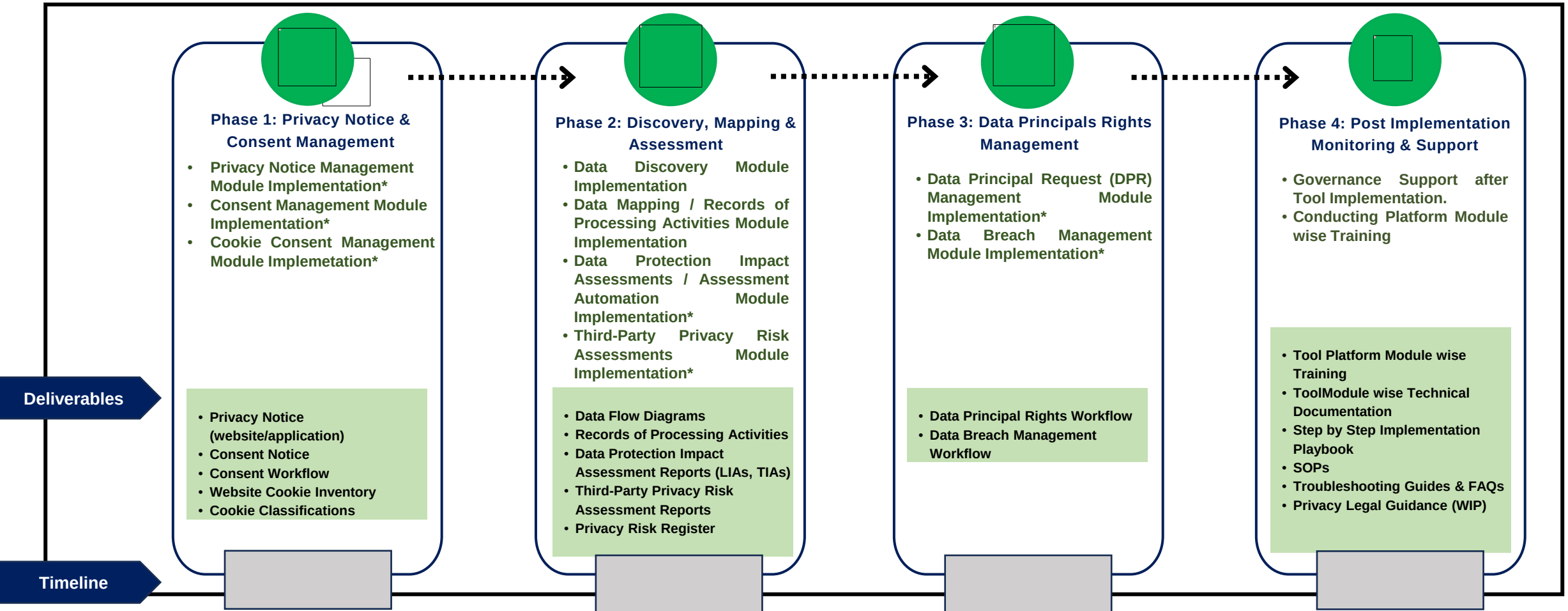


The SDC Data Landscape

One shared facility, many independent data-processing surfaces



APPROACH | DPDPA COMPLIANCE PROGRAM



**These activities could also be conducted with the support of automation capabilities*

CABINET SECRETARY CALLS FOR OVERHAUL OF DATA PRACTICES

Centre puts ministries, states on DPDP compliance clock

PRASANTA SAHU
New Delhi, August 26

THE CENTRE HAS begun pushing its own ministries, departments and state governments towards compliance with the Digital Personal Data Protection (DPDP) Act, asking them to appoint senior officials, set implementation timelines and overhaul how they collect, process and protect citizens' personal data.

In a letter to secretaries of the Government of India and chief secretaries of states and Union Territories dated August 20, Cabinet Secretary TV Somanathan has asked government bodies to prepare phased implementation plans with clearly defined responsibilities and timelines. Progress is to be reviewed periodically by the secretary or chief secretary concerned, putting responsibility for implementation directly with the administrative leadership of each ministry and state.

ONUS ON ADMINISTRATION

■ Cabinet Secretary TV Somanathan has written to GoI secretaries and chief secretaries of states and Union Territories to ensure timely implementation of Digital Personal Data Protection (DPDP) Act



■ Each ministry, department and state must designate a senior officer to oversee DPDP implementation and a nodal officer to coordinate with MeitY



■ Govt bodies must prepare phased implementation plans with defined responsibilities and timelines; review progress periodically

■ They must identify personal-data processing activities and prepare appropriate data inventories

■ Privacy notices, consent mechanisms, wherever applicable, and grievance-redressal arrangements must be reviewed

■ Capacity-building and sensitisation of officers responsible for implementing the Act must be undertaken

Somanathan has also asked each ministry, department and state to designate a senior officer to oversee implementation and nominate a nodal officer to coordinate with the Ministry of Electronics and Information Technology (MeitY), the nodal ministry for the law. "A senior officer is designated to oversee implementation of the Act" and "a nodal officer is

nominated for coordination with the Ministry of Electronics and Information Technology", he said in the letter.

The exercise will require government organisations to first establish how and where they process personal data. The Cabinet Secretary has called for identification of personal-data processing activities and preparation of appropriate data

inventories, along with a review of privacy notices, consent mechanisms wherever applicable and grievance-redressal arrangements. They will also have to strengthen technical and organisational safeguards and review contractual arrangements with third-party vendors and data processors.

Continued on Page 7



Let's Build Compliance Together

Innovate · Integrate · Transform

Thank you