



advocates & solicitors

Digital Personal Data Protection Act, 2023

A perspective on the things as they evolve
in India's data protection regime

Sajai Singh
March 8, 2024

Introduction



The Digital Personal Data Protection Act, 2023 (DPDP / Act) replaces the data protection regulations contained in the Information Technology Act, 2000 and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

DPDP heralds a slew of legislation focusing on data, digitization and online transactions, including IT rules, National Data Governance Framework Policy and a new Digital India Act.

DPDP lays down the principals, compliance and specificity to be contained in secondary / delegated legislation to follow

7 Principles of Data Economy

1

Lawful, fair and transparent usage of personal information

2

Purpose limitation; use for the purpose collected

3

Data minimization; only collect data needed, nothing else

4

Accuracy expectation; keep personal data accurate and up to date

5

Storage limitation; store till required, not perpetually

6

Security expectation; reasonable safeguards preventing data breach

7

Accountability, on the entity who decides the purpose and means of processing data

Applicability

1

Processing within India;
and outside India in
relation to offering of
goods / services in India

2

Only to personal
data in digitized
form

3

Any automated,
wholly or partly,
operations on data are
considered processing

4

Doesn't apply to publicly
available personal data;
made available by
individual or by law

5

Doesn't apply to
processing for
personal / domestic
purposes

6

Federal Government
may exclude certain
processing from Act
applicability

7

Federal Government may
also exempt certain
entities / class of entities
from Act application

Definitions

1

Data Principal

Individual to whom the Personal Data relates; if a child, includes parents or lawful guardian of the child

Akin to the concept of Data Subjects under the GDPR

2

Personal Data

Any data about an individual who is identifiable by or in relation to such data

3

Data Fiduciary

Any person who alone or in conjunction with other persons determines the purpose and means of processing of Personal Data

Akin to the concept of Data Controllers under the GDPR

4

Processing

Automated / set of operations performed on digital personal data, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use alignment / combination, indexing, sharing, disclosure, dissemination, restriction, erasure or destruction

5

Public Interest

Sovereignty & integrity of India, security of State, friendly relations with foreign States, maintenance of public order, preventing incitement to commission of any cognizable offence relating to above and preventing dissemination of false statements of fact

Grounds for Processing

1

Lawful purpose; with some legitimate use and other exceptions

2

Consent, which is free, specific, informed, unconditional and unambiguous

3

On withdrawal of consent processing to cease within reasonable time

4

Notice (precedes consent) specifies what personal data being collected, purpose and like

5

Consents prior to the Act require notification to Data Principal on processing

6

Consent Managers, registered with the DPB, may manage consent via their platforms

7

Voluntary provision of data for availing of a service may be used as such, and not otherwise

Privacy Notice

Elements

Data Fiduciaries are required to provide Data Principals with a notice stating what personal data is being collected and its purpose

- It may be important for some other information to be provided to the Data Principal, including information on third parties with whom the personal data is to be shared, to allow the Data Principal to make an informed decision

Retrospective

Notice is to be provided with retrospective effect; namely, Data Principals who have already provided consent prior to the commencement of the DPDP are to receive a notice from the Data Fiduciary within reasonable time

Consent and Non-Consensual Grounds for Processing

- All communication with Data Fiduciary in clear and plain language
- Consent should not be perpetual and irrevocable
- Concept of Post-mortem Privacy, meaning consent may be withdrawn at any time by the Data Principal
- Before data of an individual can be processed, s/he either gives consent or consent is deemed to have been given in certain circumstances, like for medical treatment, health services, disaster assistance, legal obligation, contractual obligation, vital interest, public interest, emergency response or performing a function under any law
- *Ecosystem of Consent Managers* – a platform which enables an individual to have a comprehensive view of interactions with Data Fiduciaries and consent given to them



Deemed Consent

- 'Allowed' basis of processing include:
 - Government established 'fair and reasonable' reasons for which data may be used without consent of individual
 - Government exemptions based on volume (low) or nature (low risk) of data processed by any Data Fiduciary, like start-ups
 - Research, statistical or archival processing (per demonstrable standards); not used for decision making about individual
- No employee consent required to process, if:
 - Processing for employment related activities
 - Employer protecting itself from loss / liability
 - Employee data required to enforce a legal right or in connection with a legal offence



Data Fiduciary Obligations

1

Quality Assurance:
Ensure completeness, accuracy and consistency of Personal Data they process

2

Data Breach Notification: Need to go to the Board and all affected Data Principals; without any prescribed thresholds

3

Safeguards / Security Measures: Technical / organizational safeguards and reasonable security measures to ensure protection of Personal Data / avoiding data breaches

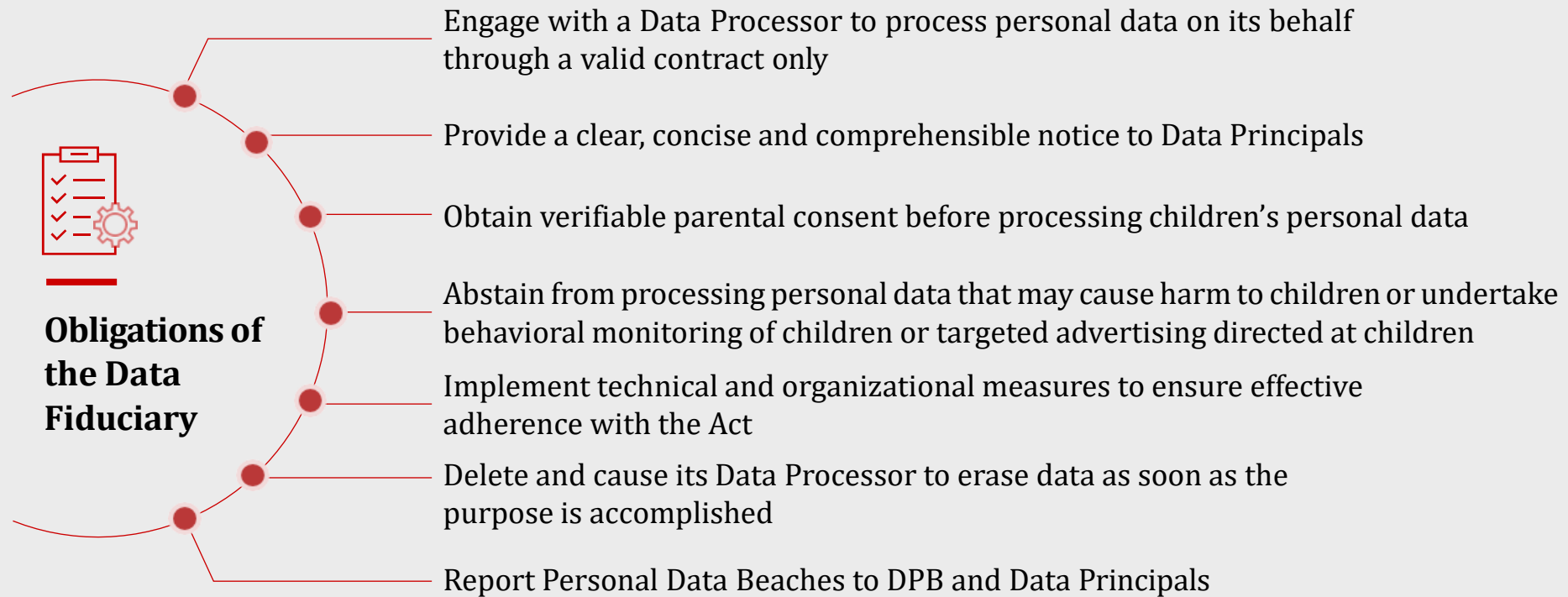
4

Retention: Personal data may not be retained beyond the purpose for which it was collected or after consent is withdrawn by the Data Principal

5

Redressal Person: Grievance Office (DPO's in certain situations) details to be made known to Data Principals

Obligations Summary



Exemptions

Applicable to Data Fiduciary from obligations (except for being responsible for its data processor and taking reasonable security safeguards)



Processing for enforcing any legal right or claim



Processing for performance of any judicial or quasi-judicial functions by any Indian court / tribunal or other body



Processing in the interest of prevention, detection, investigation or prosecution of any offence of any law



Processing of Data Principals outside the territory of India pursuant to any contract entered into with any person outside the territory of India by any person based in India



Processing necessary for a merger / amalgamation or similar arrangement as approved by a court or other authority competent

Significant Data Fiduciary

- Federal Government may notify any Data Fiduciary (on a stand-alone factor) or a class of Data Fiduciaries as Significant Data Fiduciary (SDF)
 - based on volume / amount and sensitivity of Personal Data processed, potential influence on the sovereignty and integrity of India, risk of harm to Data Principal, threat to India's democracy, security of State, public order and other similar concerns
- SDF's need to fulfill certain additional obligations for greater security
 - *Appoint an Independent Data Auditor, to evaluate SDF's compliance under the Act*
 - *Conduct Data Protection Impact Assessment, covering a description of Data Principal rights, processing purpose, an assessment and management of risk to such rights*
 - *Appoint a Data Protection Officer (DPO) based in India, to serve as point of contact for grievance redressal; being responsible to senior leadership of SDF*



Data Processors

Appointment

A Data Fiduciary may appoint a Data Processor to process personal data for them; this relationship needs to be based on a valid contract covering the passing of obligations to the Data Processor, including putting in place reasonable security practices and procedures, data breach notification requirement and cross border data restrictions, as applicable

Responsibility

A valid contract or any other relationship structure doesn't absolve the Data Fiduciary of its own obligations under the DPDP or penalties applicable for non-compliance

Rights of Data Principal

Usually related to consent-based processing; not on legitimate use processing

Grievance Redressal: The Data Fiduciary is required to respond to grievance of Data Principal within 7 days or shorter period that may be prescribed; this right may also be redressed against a Consent Manager

Access & Erasure Rights: To correct, update, complete and erase Personal Data

Information Right: A Data Principal has the right to obtain information regarding the categories of Personal Data being processed and identities of all the Data Fiduciaries with whom the Personal Data has been shared

Nomination Right: The Data Principal may nominate a representative in case of incapacity or death of the Data Principal, to exercise their rights under the Act

Data Portability: Unfortunately, the Act does not provide the right to data portability to Data Principal; thus, a Data Principal will not be able to extract data related to him/her from one data silo and move to another

Right to be Forgotten: Not provided for in the DPDP, thus the Data Principal cannot ask the Data Fiduciary to stop disclosing their personal information – *erasure only option*

Duties of Data Principal

Comply with all applicable laws, while exercising rights under DPDP

Not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board

Not to furnish false particulars or suppress any material information or impersonate another person

Only furnish such information as is verifiably authentic while exercising right to correction or erasure



Personal Data of Children and People with Disabilities

Verifiable parental consent required before processing Personal Data; though consent will not allow certain processing, tracking or advertising

DPDP prohibits tracking or behavioral monitoring or any activity that is likely to have a detrimental effect on the well-being of a child

Targeted advertising of children not allowed

Exceptions may be allowed by the Federal Government, specially where the Data Fiduciary demonstrates verifiable safe processing of such data



Data Protection Board (DPB)

With appeal before the Telecom Disputes Settlement and Appellate Tribunal
(then the SC)

1

Enforcing compliance;
including referring matters to mediation

2

Imposing penalties / taking action for non-compliance (no civil court may entertain any matter under the DPDP)

3

Issuing directives to Data Fiduciaries, including to remedy breaches regarding Personal Data

4

Conduct inquiries

5

Everyone needs to follow directions of the DPB, following authority given under the Act

Breach Notification

Personal Data Breach

Personal Data Breach includes any unauthorized processing of personal data, accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data that compromises the confidentiality, integrity, or availability of such data

- No materiality or sensitivity threshold has been prescribed

Notification Requirements

In the event of a data breach, the Data Fiduciary and Data Processor are obligated to notify each affected Data Principal (and DPB); in addition to any other notification requirement (like CERT-In, IRDAI, Stock Exchanges, SEBI, RBI, MCA, etc.)

- No time has been prescribed in which the Data Fiduciary is required to inform the DPB and Data Principals regarding data breach

Data Protection Impact Assessment

A process comprising description, purpose, assessment of harm, measures for managing risk of harm and such other matters with respect to processing of Personal Data, as may be prescribed



Cross Border Data Transfer

Cross-border data transfer easy, allowing Data Fiduciaries to freely transfer Personal Data to other countries

Personal Data may not be transferred to notified (blacklisted) countries and territories (to be notified by the Federal Government)

Since there is no concept of data localization; the requirement to store Personal Data within India does not exist under the DPDP; though it may exist to some sets of data, which *may* include personal data, under other statutes



Penalties

Data Principals may not seek compensation from Data Fiduciaries for damages incurred due to unlawful processing

If non-compliances are significant (say not maintaining adequate security safeguards), following principles of natural justice, the Board may impose a financial penalty not exceeding INR 250 Crore (US\$ 30 Million) in each instance

While the Federal Government may enhance the penalties; they cannot surpass twice the numbers presently prescribed (therefore INR 500 Crore / US\$ 60 Million)



Considerations before awarding a Penalty

Consideration would be given to the following, while imposing the penalty:

- Nature, gravity and duration of non-compliance;
- Type and nature of the Personal Data affected by the non-compliance;
- Repetitive nature of the non-compliance;
- Whether, the person, as a result of non-compliance, has realized a gain or avoided a loss;
- Whether the person took any action to mitigate the impact of non-compliance, its timeliness and effectiveness;
- Whether the penalty is proportionate and effective; and
- Likely impact of the imposition of the financial penalty on the person



Other Interesting Provisions

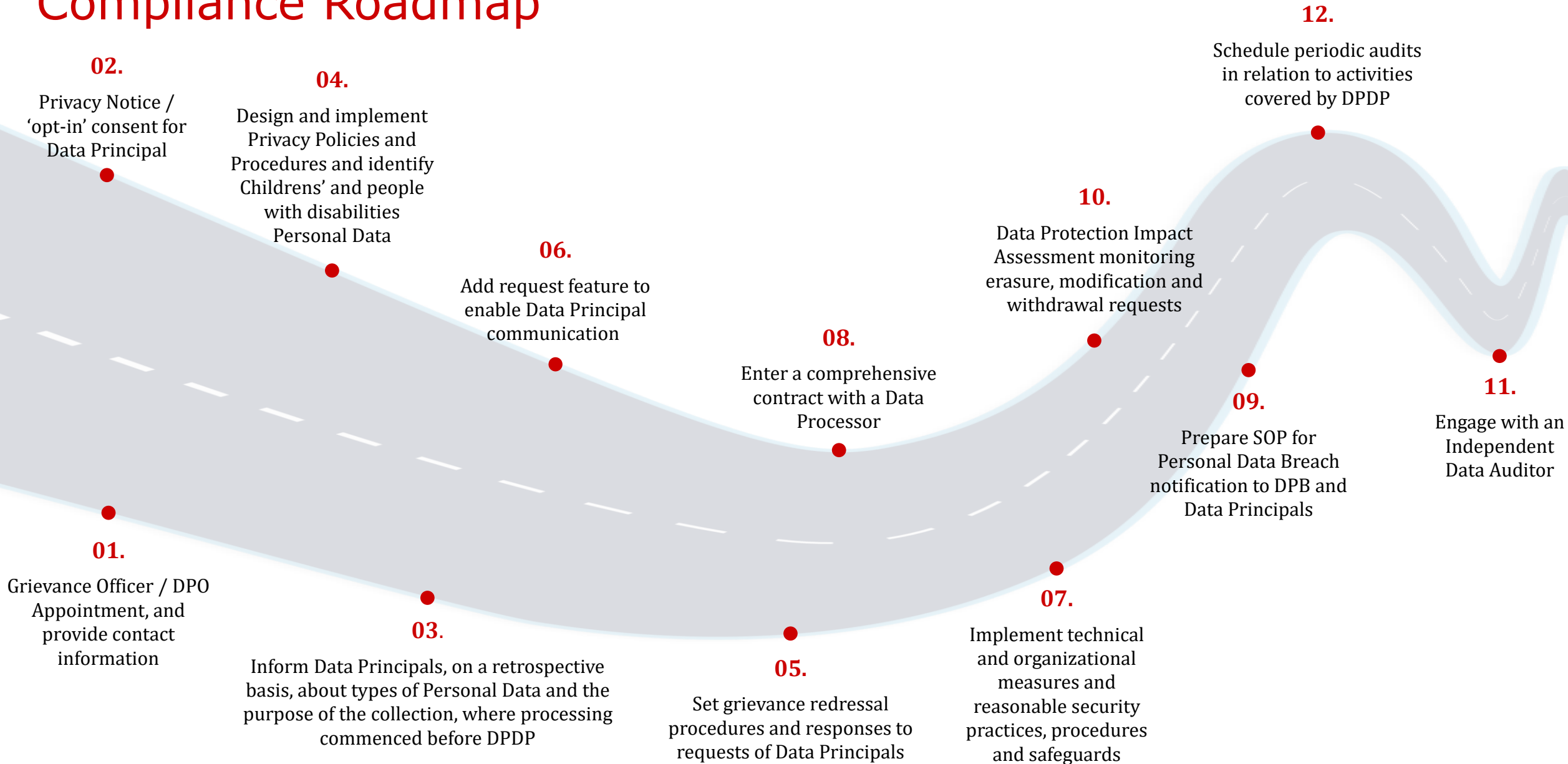
- Federal Government may order intermediaries (cloud service providers / ISPs) to block access to information contained in any computer resource
- Contravening parties may, at any stage of proceedings before the Board, voluntarily admit non-compliance and undertake to adopt rectification measures – thus obtaining immunity from further proceedings
- The Government will become India's major Data Fiduciary as it processes Personal Data of millions of people for services, benefits, granting of permits, licenses and official ID's and law enforcement
- No provision regarding privacy by design and default
- Devil will be in the detail contained in delegated legislation



Issues to Consider Right Away

- Get familiar with the law
- Conduct a comprehensive data inventory / mapping exercise using data discovery techniques
- Develop mechanisms to provide notices to Data Principals on Personal Data collected previously and going forward
- Implement a consent management mechanism to collect, maintain, track, and update consent from individuals
- Establish and maintain reasonable technical and organizational security measures to protect Personal Data
- Consider 'opt-in' consent for all Personal Data collected
- Add a 'request's' feature to website / platform / application to allow easy access to Data Principal communications, requests and grievances
- Set an internal protocol to respond to grievances, requests and other Data Principal communications - *including of employees*
- Monitor erasure and withdrawal requests and erase using globally accepted standards of secure erasure
- Implement tools to track modifications to databases, to maintain quality, consistency and integrity of Personal Data
- About Childrens' data, identify processing activities that need to cease, like product recommendations, and cease them
- Create and implement SOP for breach identification, reporting, mitigation and regular audits on systems
- Review Data Processing Agreements with clear covenants on breach responses, security standards and cross-border data flow
- Access the ability to translate (from English) to 22 Indian languages of any Data Principal facing document

Compliance Roadmap



Thank You



Sajai Singh
Partner, JSA
sajai@jsalaw.com
+91-98450 78666



Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi

This presentation is not an advertisement or any form of solicitation and must not be construed as such. This presentation has been prepared for general information purposes only. Nothing in this presentation constitutes professional advice or a legal opinion. You should obtain appropriate professional advice before making any business, legal or other decisions. While endeavours have been made to keep the information updated, JSA makes no representations or warranties regarding the completeness, accuracy and reliability of such information. Any onward distribution of this presentation must be with the prior consent of JSA. JSA and the presenters also disclaim all and any liability to any person who takes any decision based on this presentation.

Copyright © 2023 JSA | all rights reserved