Protection of Personal Data Bill, 2018

DSCI
PROMOTING DATA PROTECTION

NASSCOM®

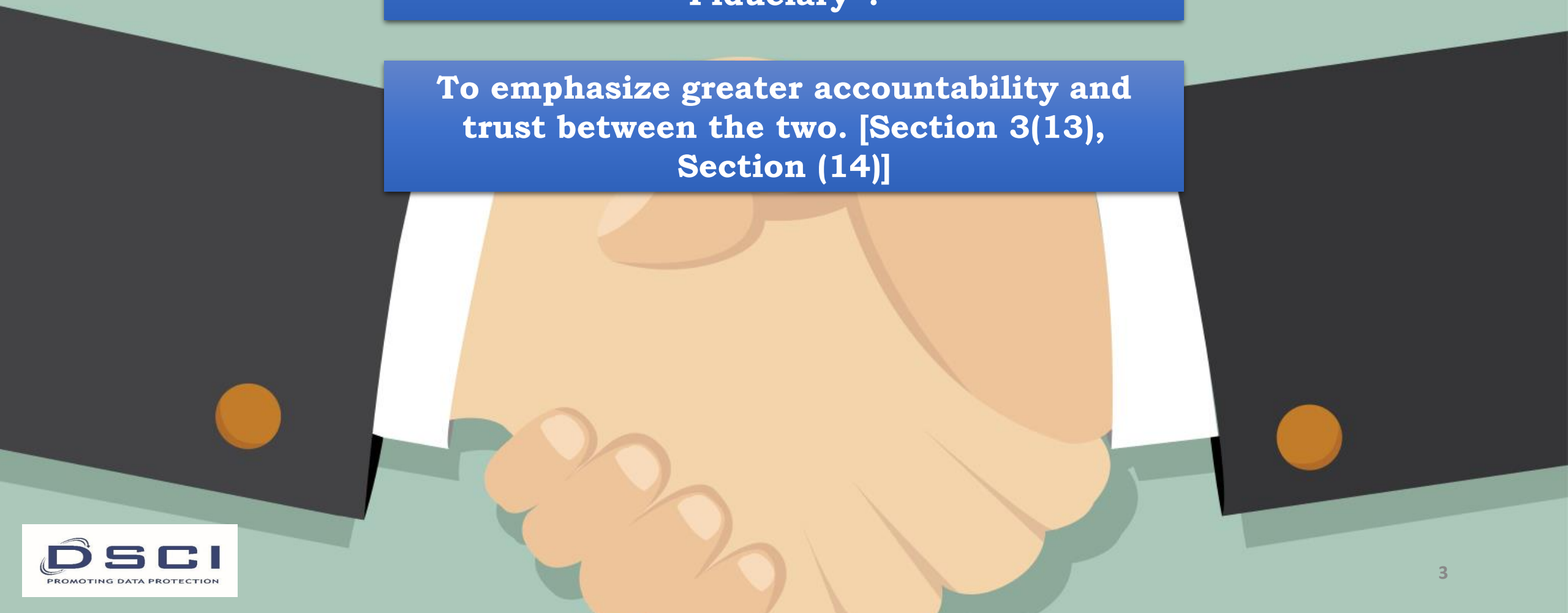
Salient Features

DSCI
PROMOTING DATA PROTECTION

Data Principal and Data Fiduciary

The known terms of references, i.e., "Data Subject" and "Data Controller", have been reformulated as "Data Principal" and Data Fiduciary".

To emphasize greater accountability and trust between the two. [Section 3(13), Section (14)]



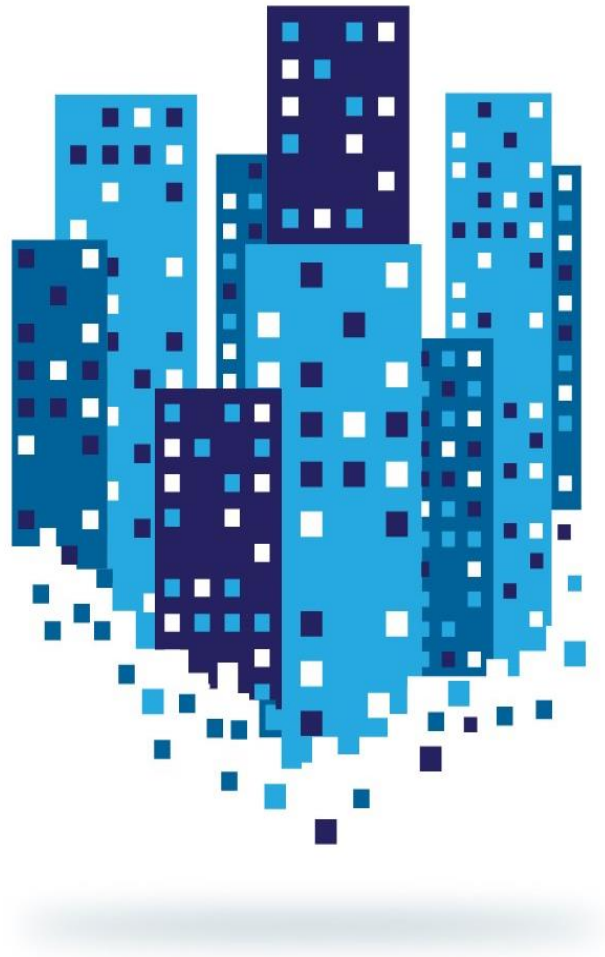
DSCI
PROMOTING DATA PROTECTION

Territorial Scope

Processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India; and

Processing of personal data by the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law.

Central Government may exempt from the application of this Act or any provisions of this Act, processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.



DSCI
PROMOTING DATA PROTECTION

Extraterritorial Scope

Data fiduciaries or data processors not present within the territory of India, if they carry out processing of personal data in connection with any business carried on in India

Systematic offering of good and services to data principles in India

Any activity which involves profiling of data principals within the territory of India.

Personal Data

Personal data has been defined on the parameters of identifiability. Any characteristic, trait, attribute or any combination thereof that directly of indirectly identify a natural person.

The definition does not specifically mention any particular form of data or attribute.

De-identified data (i.e., data that cannot be attributed to an individual without the use of additional information) is personal data.

Anonymized data is not personal data.

DSCI
PROMOTING DATA PROTECTION

Personal Data: Scenarios

Identified Individual

Asylum seekers hiding their real names in a sheltering institution have been given a code number for administrative purposes.

That numbers serve as an identifier, so different pieces of information concerning the stay of the asylum seeker in the institution are attached to it.

The code number has a close and immediate connection to the physical person, thus allowing him to be distinguished from other asylum seekers.

The code can be used to attribute different pieces of information to him, making him an "identified" natural person.

Personal Data: Scenarios

Identifiable Individual

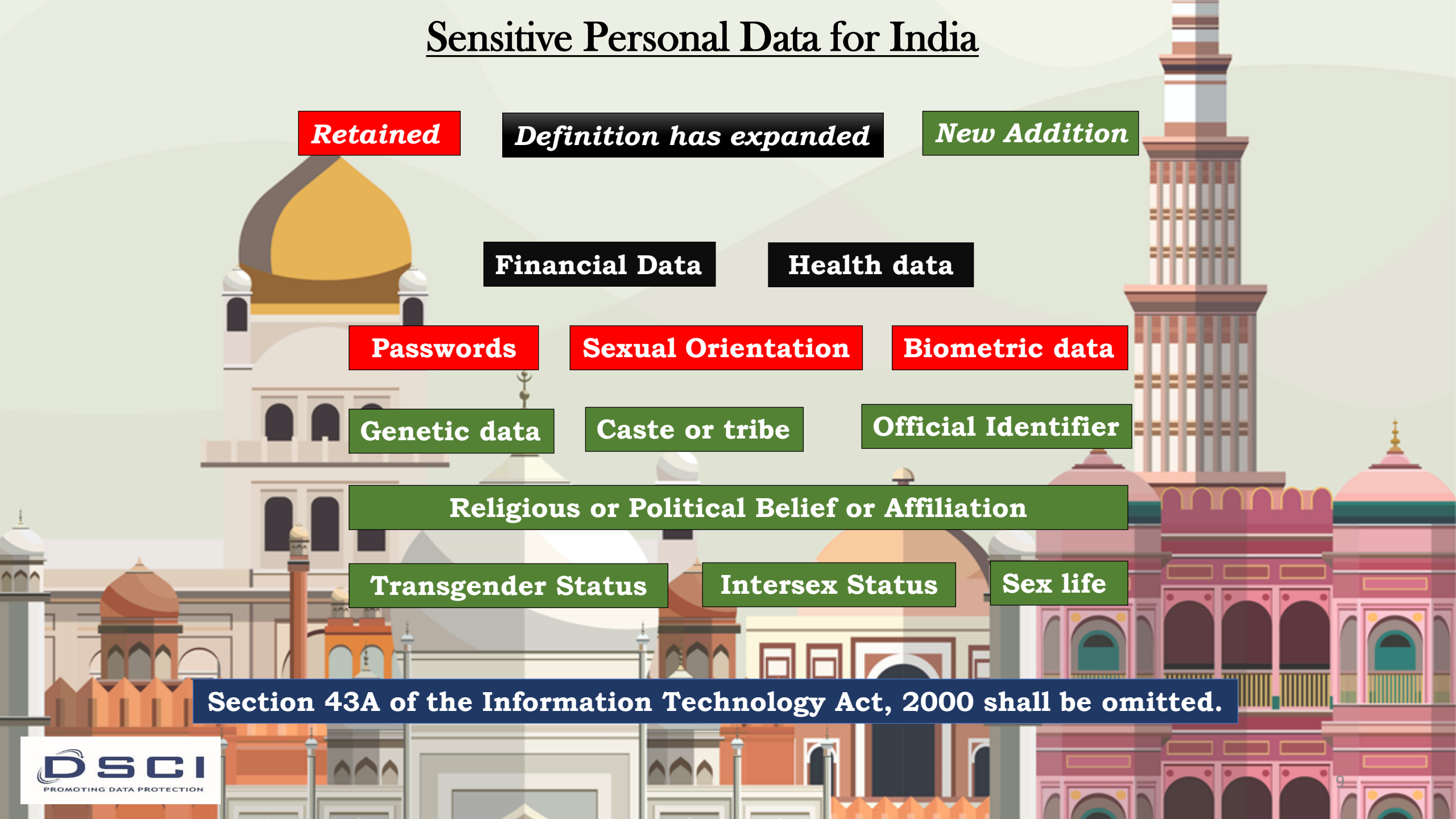
Information is published about a former criminal case which won much public attention in the past.

In this publication there are no traditional identifiers especially no name or date of birth of any person involved.

It does not seem unreasonably difficult to gain additional information allowing one to find out who the persons mainly involved are, e.g. by looking up newspapers from the relevant time period.

It seems therefore justified to consider the information in the given example as being 'information about identifiable persons' and as such 'personal data'.

Sensitive Personal Data for India



DSCI
PROMOTING DATA PROTECTION

Sensitive Personal Data

Financial Data

Under SPDI Rules, 2011, financial information included information such as bank account or credit card or debit card or other payment instrument details.

Under PPDB, 2018, the definition of "Financial data" has been broadened to include any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history.

Sensitive Personal Data

Health data

The definition under PPDB, 2018, covers Physical, Physiological and Mental Health condition and Medical records and history, as mentioned under SPDI rules, 2011, while broadens the definition to include other parameters as well.

"Health data" means data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services.

Data Principal Rights

- **Right to Confirmation and Access**
- **Right to be Forgotten**
- **Data Portability**
- **Correction**

Data Principal Rights

Request to be made in writing to the data fiduciary with reasonable information to satisfy the data fiduciary of the identity of the data principal making the request and

Data fiduciary shall acknowledge receipt of such request within such period of time as may be specified.

The data fiduciary may charge a reasonable fee to be paid for complying with requests

Except for requests made under clauses (a) and (b) of sub-section (1) of section 24 (Access and confirmation) and section 25 (Correction) which shall be complied with by the data fiduciary without charging any fee.

DSCI PROMOTING DATA PROTECTION

Transparency and Accountability

- Significant Data Fiduciaries
- Guardian Data Fiduciaries
- Data Protection officer
- Data Audits
- Data Protection Impact Assessment
- Record Keeping
- Privacy by Design
- Grievance Redressal

Significant Data Fiduciaries

The authority shall classify a data fiduciary as a significant data fiduciary.

The classification is subject to:
(a) Volume of personal data processed
(b) Sensitivity of personal data processed
(c) Turnover of the data fiduciary
(d) Risk of harm from processing
(e) use of new technologies for processing
(f) any other relevant factor

Significant data fiduciaries must perform: data protection impact assessments, record-keeping, subject to data audits, appoint data protection officer and are subjected to mandatory registration with the authority.

Guardian Data Fiduciaries

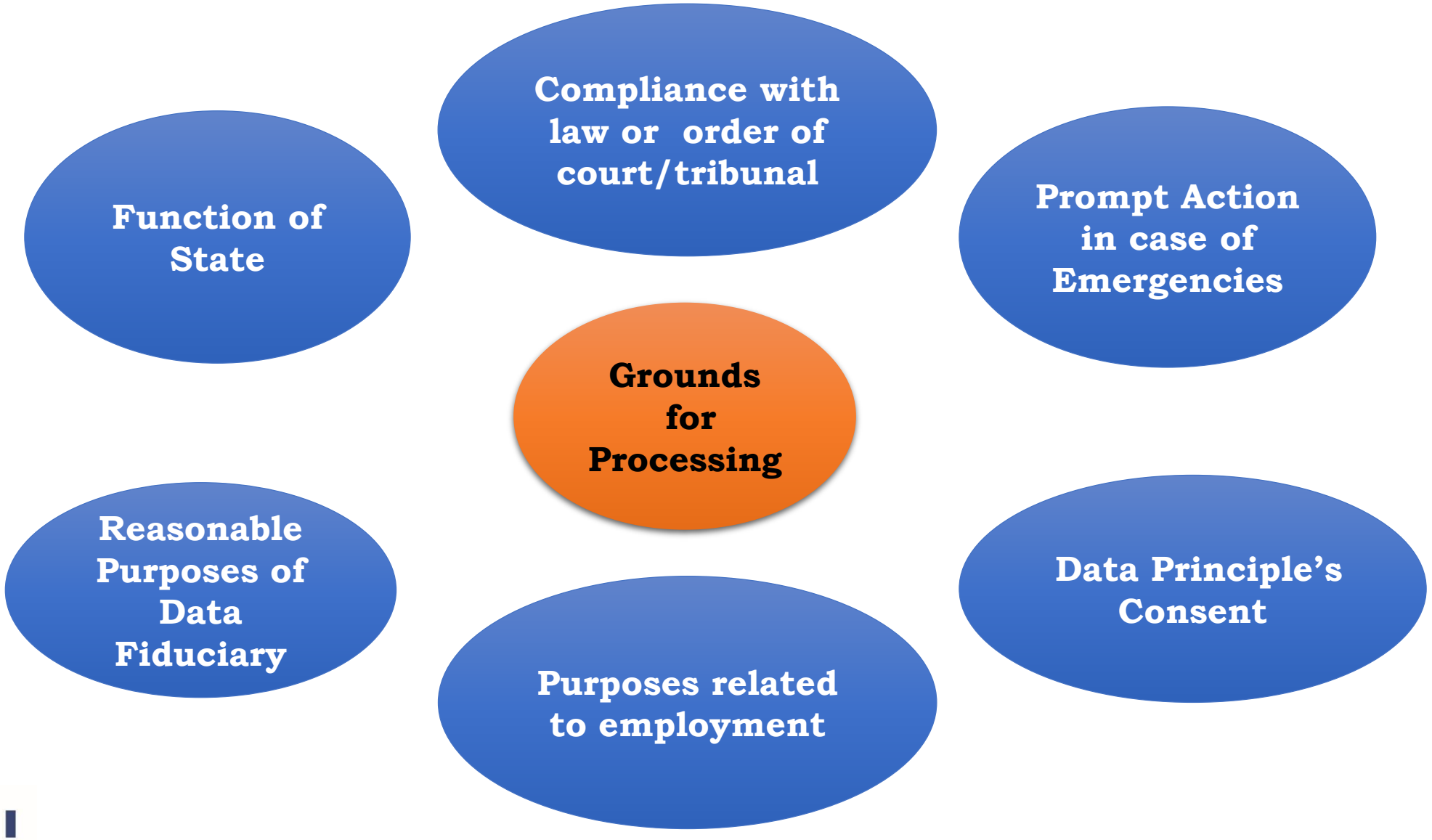
The authority shall notify particular fiduciaries as guardian data fiduciaries.

The classification is subject to:
(a) data fiduciaries who operate commercial websites or online services directed at children; or
(b) data fiduciaries who process large volumes of personal data of children.

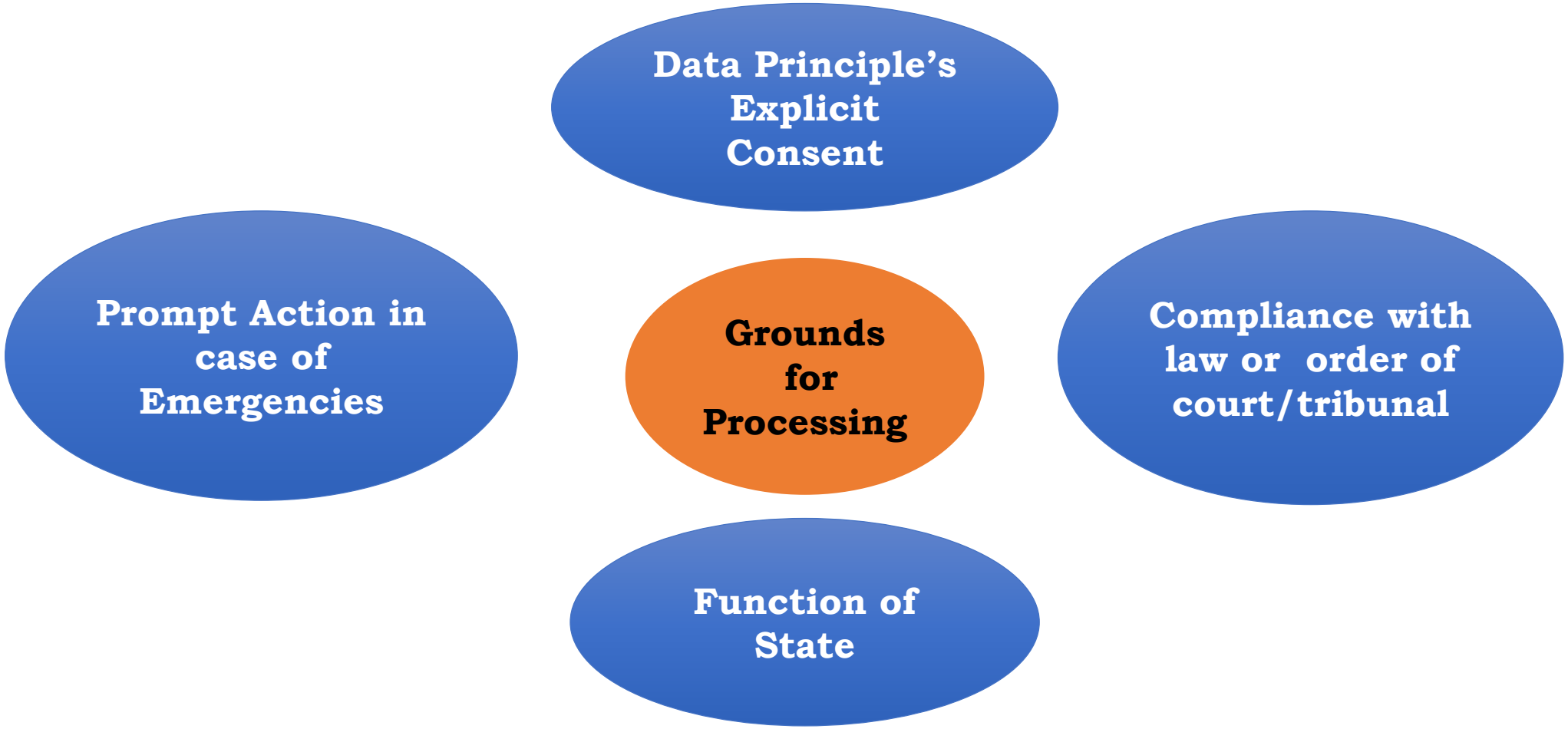
They shall be barred from profiling, tracking, behavioural monitoring , or targeted advertising directed at children and undertaking any other processing of personal data that can cause significant harm to the child.

DSCI
PROMOTING DATA PROTECTION

Grounds for Processing Personal Data



Grounds for Processing Sensitive Personal Data



Prompt action in case of emergencies is restricted to passwords, financial data, health data, official identifiers, genetic data, and biometric data.

Processing by entities other than data fiduciaries

The data fiduciary shall only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid contract.

The data processor shall not further engage, appoint, use, or involve another data processor in the relevant processing on its behalf except with the authorisation of the data fiduciary, unless permitted through the contract.

The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary and treat any personal data that comes within their knowledge as confidential.

Restrictions on Transfer of Personal Data Outside India:

Storing one serving copy of all personal data within the territory of India.

Central government may classify any sensitive personal data as critical personal data and mandate its storage and processing exclusively within India.

Exceptions for transfer of Critical Personal Data Outside India:

Critical Personal data may be transferred to a particular person or entity engaged in the provision of health services or emergency services where such transfer is strictly necessary for prompt action. Such transfer needs to be notified to the authority within a prescribed period.

Critical Personal data maybe transferred to a particular country, a prescribed sector within a country or to a particular international organisation that has been prescribed by the Central Government.

DSCI PROMOTING DATA PROTECTION

Conditions for Cross-Border Transfer of Personal Data

(a) Standard contractual clauses or intra-group schemes approved by the authority

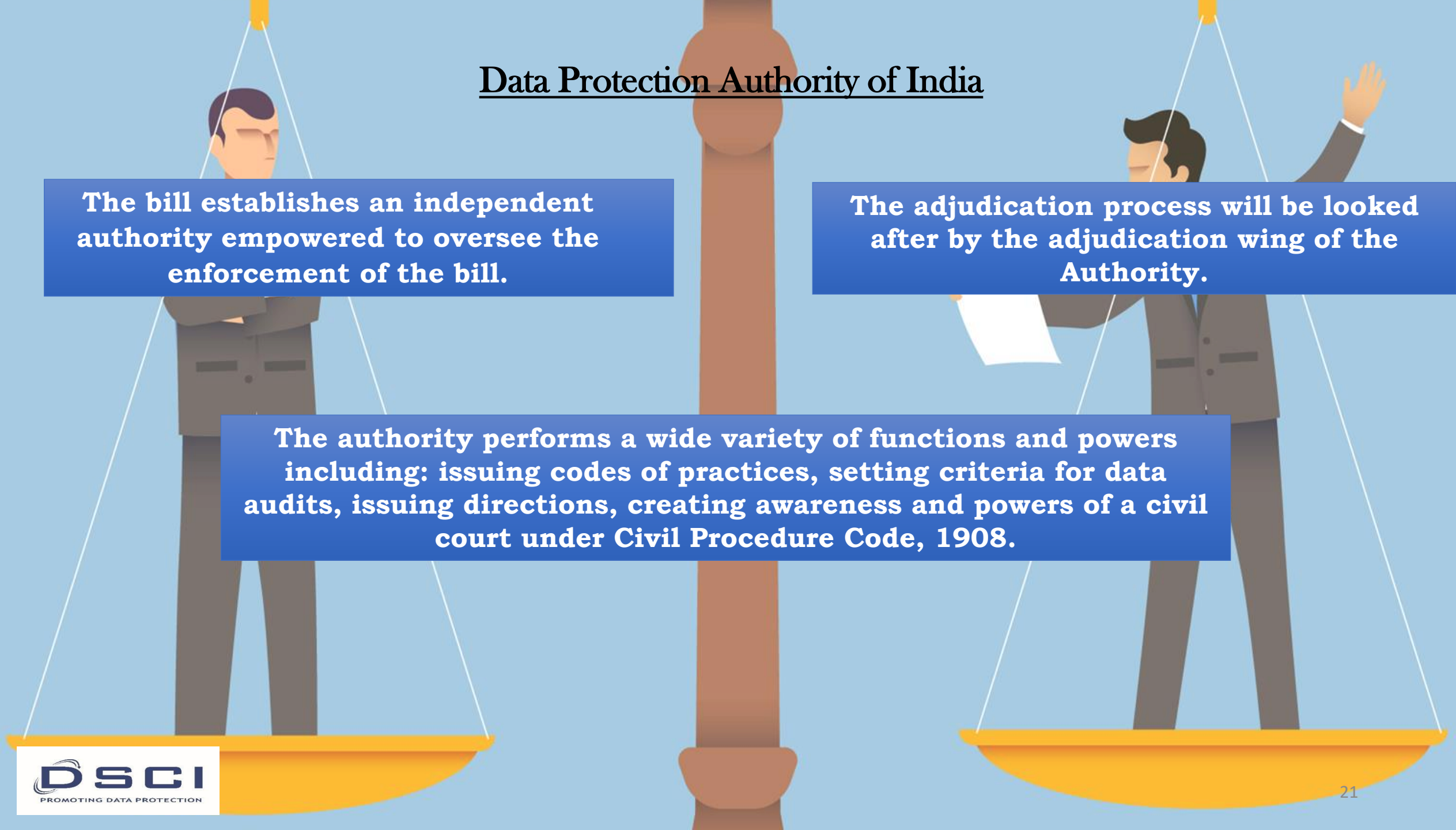
(b) Adequacy determination by Central Government of a country, sector or international organisation

(c) Transfers permissible for prompt action

(d) Data principal has consented to transfer of personal data in addition to (a) or (b).

(e) Data principal Explicitly consented for transfer of sensitive personal data (not categories as critical) in addition to (a) or (b).

Data Protection Authority of India



The bill establishes an independent authority empowered to oversee the enforcement of the bill.

The adjudication process will be looked after by the adjudication wing of the Authority.

The authority performs a wide variety of functions and powers including: issuing codes of practices, setting criteria for data audits, issuing directions, creating awareness and powers of a civil court under Civil Procedure Code, 1908.

DSCI
PROMOTING DATA PROTECTION

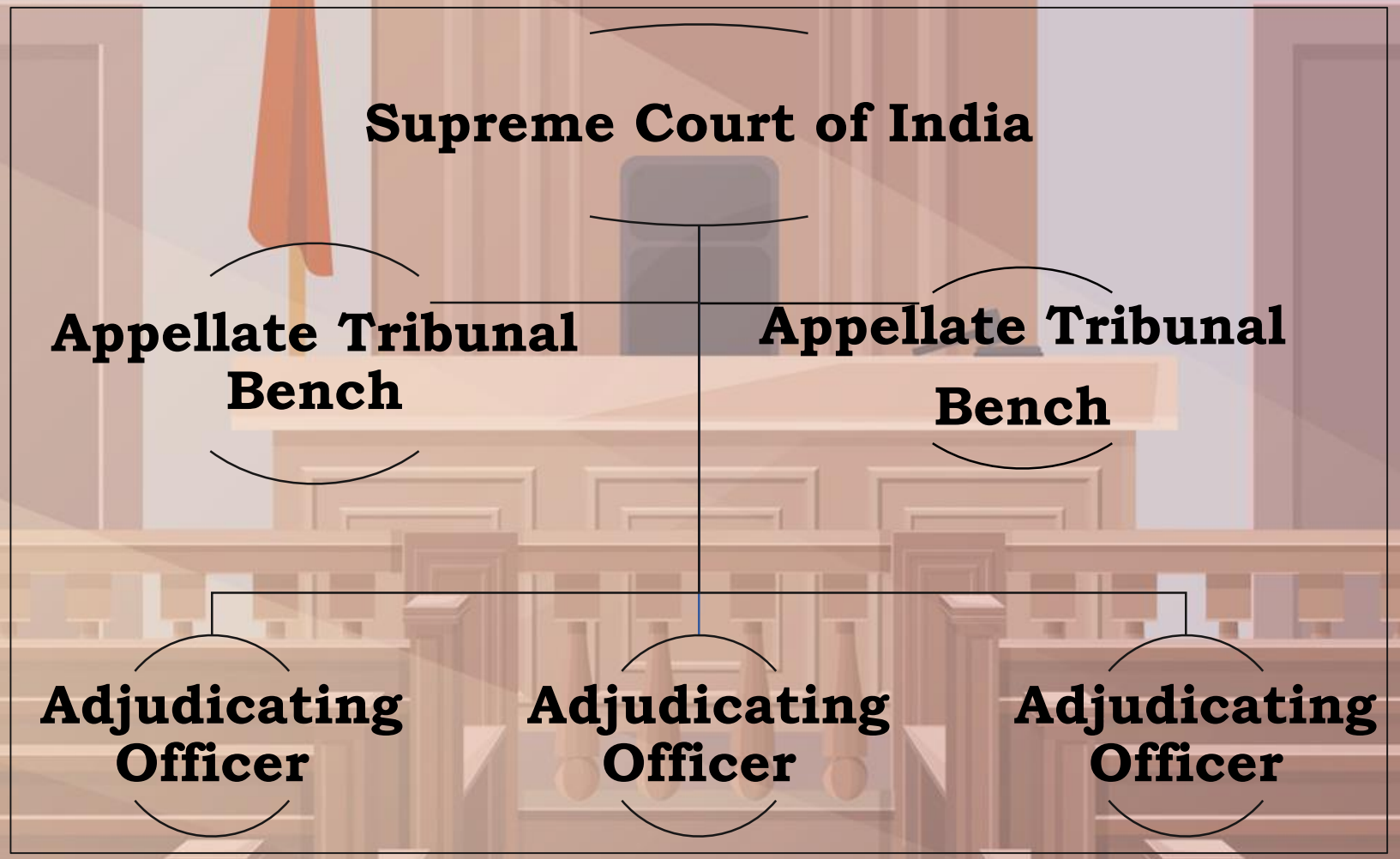
Penalties, Remedies and Offences

Penalties ranging from five crore rupees or two per cent of total worldwide turnover to fifteen crore rupees or 4% of the total worldwide turnover.

The Data principle under section 75 has the remedy to claim compensation for harm suffered as a result of any violation of any provision in the bill from the data fiduciary or the data processors.

The bill inscribes certain offences under chapter XIII of the bill, which are punishable with imprisonment.

Adjudication Structure

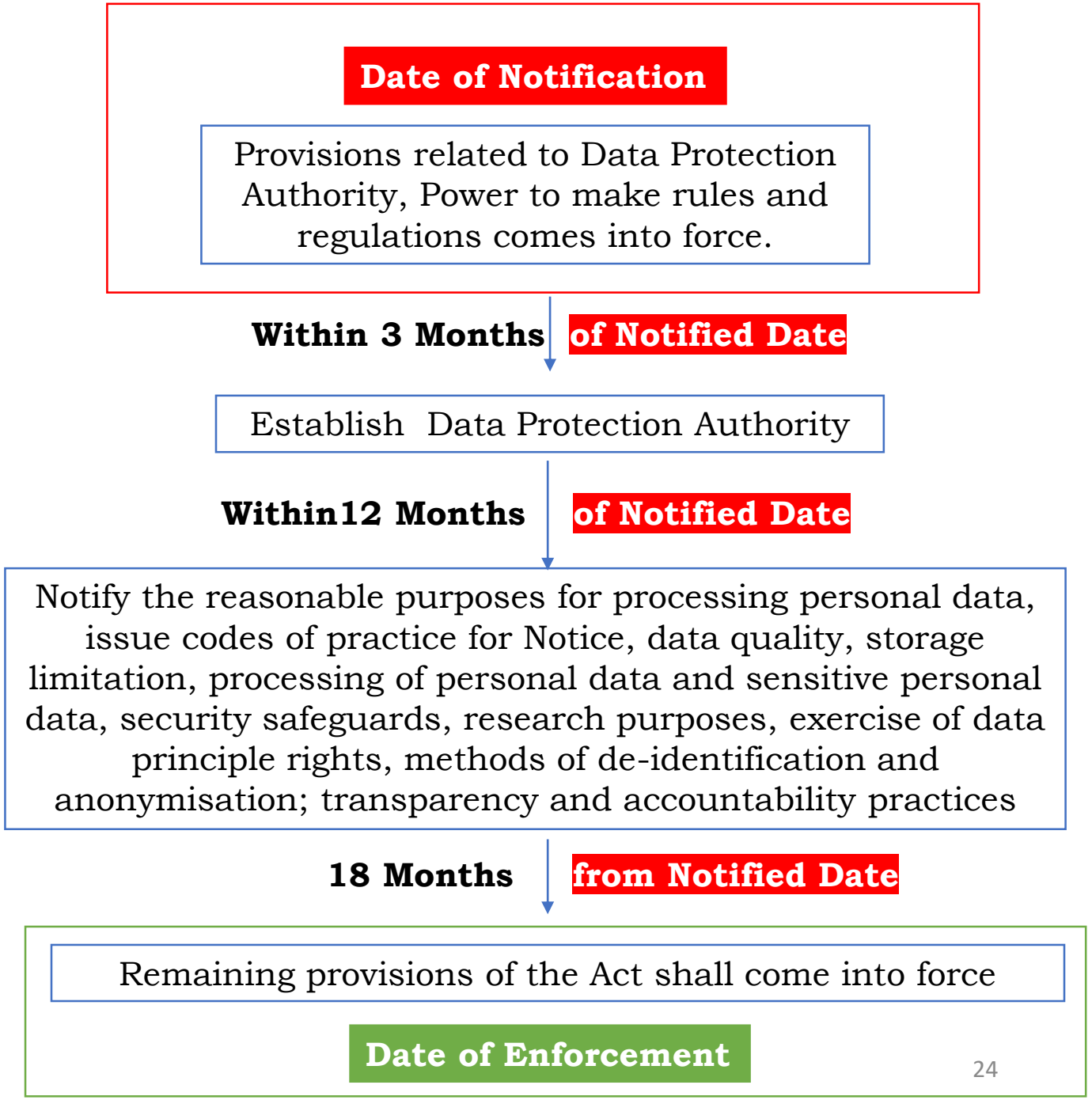


DSCI
PROMOTING DATA PROTECTION

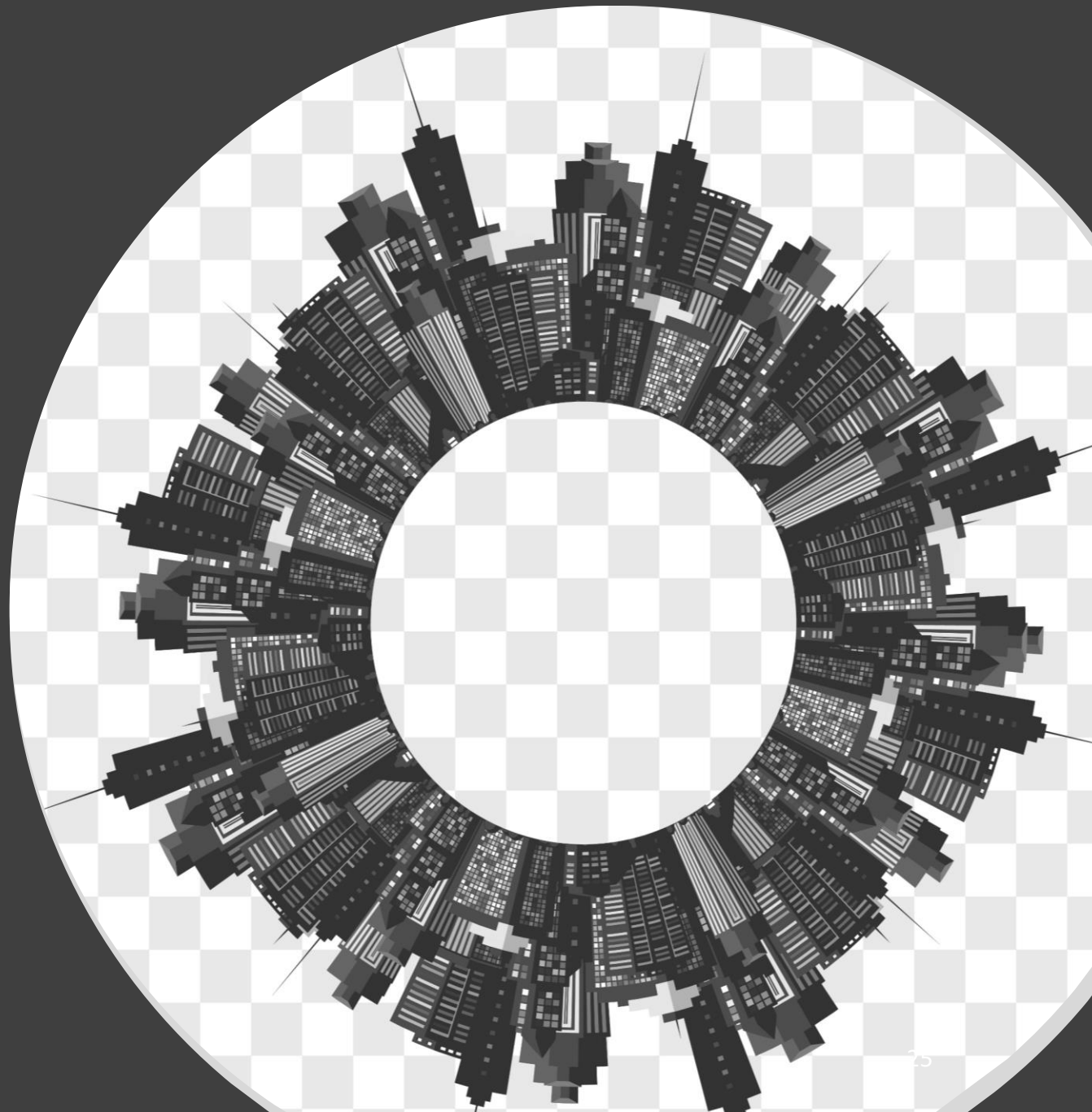
Transitional Provisions

The date of notification shall be within 12 months from the date of enactment of the act. Refer the diagram for the timeline to follow.

The date of enforcement of section 40 (restrictions on cross-border transfer of personal data would be notified by the central government.



Major Impact Areas for Industry



DSCI
PROMOTING DATA PROTECTION

Restrictions on Transfer of Personal Data Outside India

A copy of all personal data is required to be stored in India

Sensitive personal data as critical personal data and mandate its storage and processing exclusively within India.

Adverse effects

Security Challenges

Operational Challenges

Barriers for Global Trade

Cost Implications

DSCI PROMOTING DATA PROTECTION

Conditions for Cross-Border Transfer of Personal Data

Standard contractual clauses or intra-group schemes approved by the authority and adequacy determination are the only effective available options for cross-border transfers.

Conditions like consent/explicit consent are not stand alone grounds for cross-border transfer.

Control exercised by the authority and central government borders on intrusive.

Adverse Effects

Barriers for Global Trade

Heavily Bureaucratic Structure

Departure from global best practices

DSCI PROMOTING DATA PROTECTION

Heavy Cost of Compliance

Granular compliance requirements would significantly increase cost of compliance.

Especially for organisations classified as significant data fiduciaries.

Adverse Effects

Impact on existing business processes

Impact on SMB and Start Up Segment

DSCI PROMOTING DATA PROTECTION

Offences by Companies

In case of offence committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Where an offence under has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Adverse Effects

Impact on India's Image as a destination for investment

Instances of Misuse

Overregulation of Industry

Transitional Provisions

18 months transitional period is insufficient to meet the granular requirements laid down by the law.

Adverse Effects

Lack of certainty over the localisation requirements

Would lead to rushed implementation

Thank you!