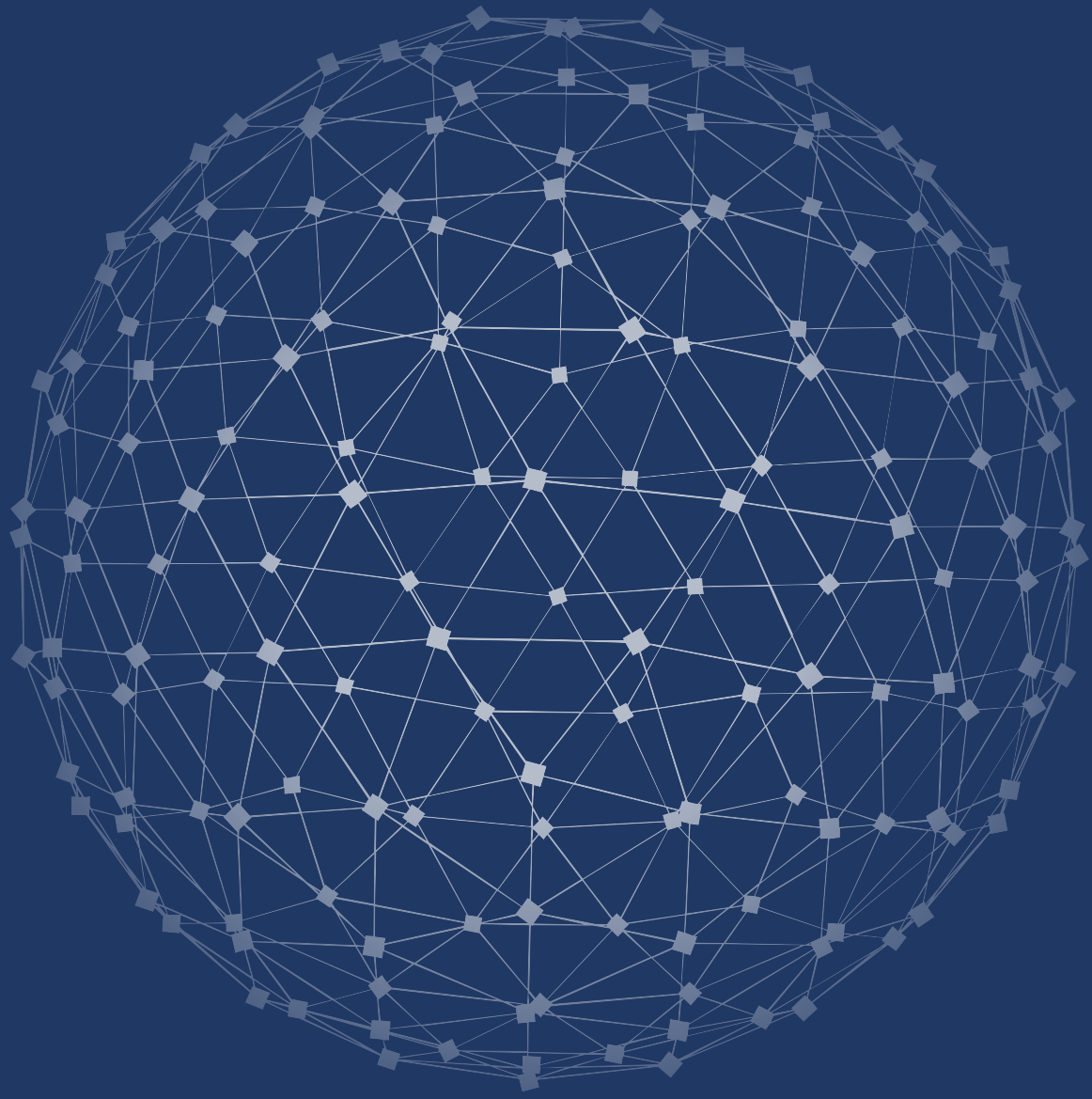
DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

NASSCOM®

Personal Data Protection Bill, 2019



Introduction

NASSCOM®

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Justice K S Puttaswamy v. Union of India	• Unanimous view that Right to Privacy is a **fundamental right under Article 19, 21, 20(3), 25.** • Existence of Informational Privacy expressly recognised.
Justice Srikrishna Data Protection Committee	Set up under the Chairmanship of Former Supreme Court Justice B.N. Srikrishna to study various issues relating to data protection in India, make specific suggestions on principles underlying a data protection bill and draft such a bill.
Draft Protection of Personal Data Bill, 2018	• The bill went through a public consultation process. • Ownership of the bill was transferred to the Ministry of Electronics and Information Technology, to be tabled in the parliament.
Protection of Personal Data Bill, 2019	• PDP Bill, 2019 now stands referred to a Joint Parliamentary Committee (**JPC**) of both houses of the Parliament, chaired by Smt. Meenakshi Lekhi, Member of Parliament. The JPC will be submitting its report on the PDP Bill, 2019 in the last week of the Budget Session of the Parliament in 2020, after due consultation with stakeholders.

Context: Territorial & Extraterritorial Scope

NASSCOM® DSCI PROMOTING DATA PROTECTION A NASSCOM® Initiative

Territorial

Processing of Personal Data

- collected, disclosed, shared within India
- by State, Company, Indian citizen or body of persons incorporated under Indian law

Extraterritorial

Processing of Personal Data for

- Systematic activity of offering goods or services to data principals within the territory of India;
- in connection any business carried on in India
- any activity which involves profiling of data principals within the territory of India

Central Government ***may*** exempt from the applicability of this law the processing of personal data of data principals who are not within the territory of India, pursuant to any contract

Context: Change in terminology

NASSCOM®

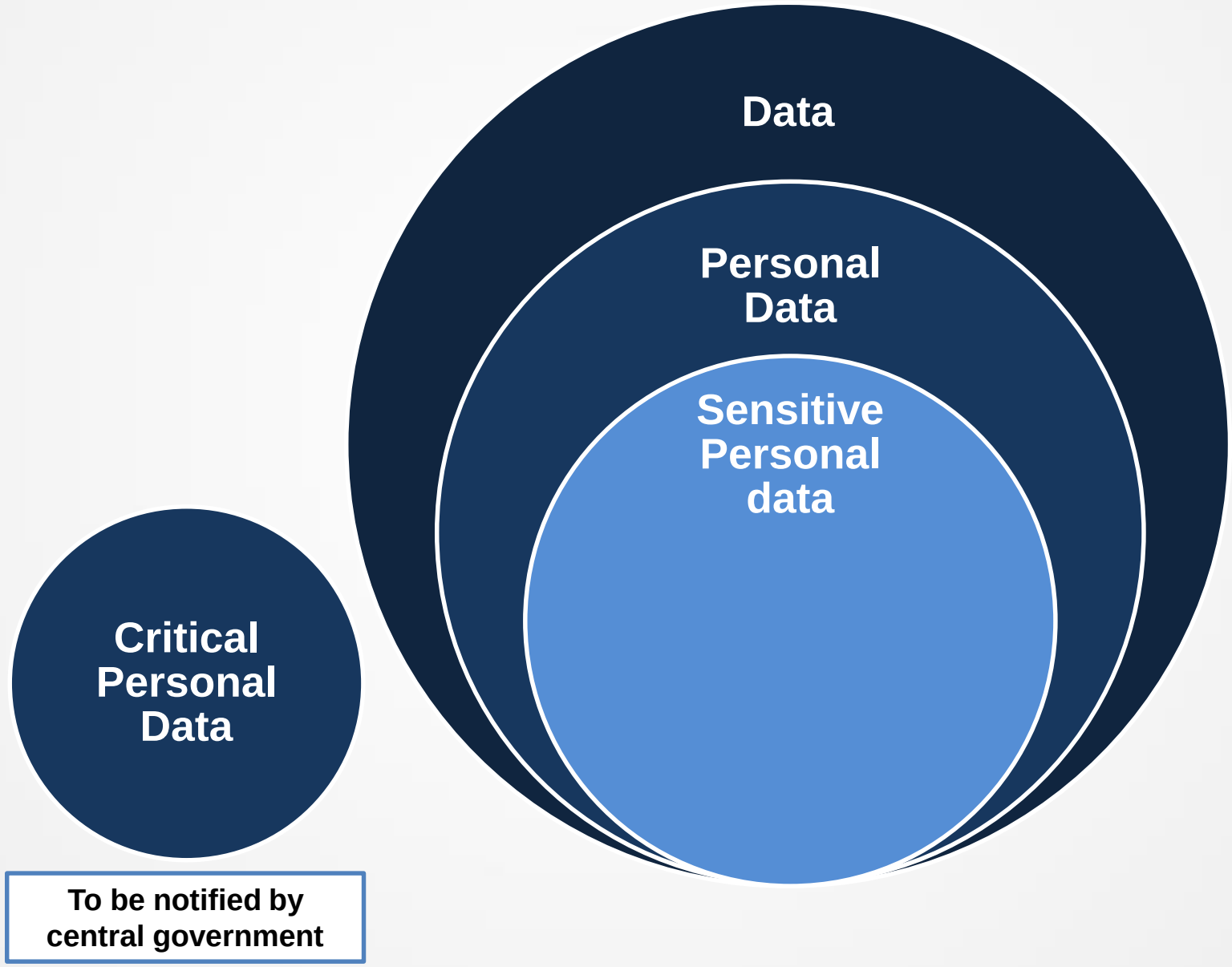
DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

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.

Context: Data Classification



A. Personal Data

Data about or relating to a natural person who is directly or indirectly identifiable

Any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information

Shall include any inference drawn from such data for the purpose of profiling

Annoymised data is not personal data.

B. Sensitive Personal Data

NASSCOM®

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

EU General Data Protection Regulation

- Racial or Ethnic Origin
- Political beliefs
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data
- Physical or mental health
- Sex life or Sexual orientation

Indian Protection of Personal Data Bill, 2019

- Financial data;
- Health data;
- Official identifier;
- Sex life;
- Sexual orientation;
- Biometric data;
- Genetic data;
- Transgender status;
- Intersex status;
- Caste or tribe;
- Religious or political belief or affiliation

Geographical Similarities

Geographical Variations

SPDI Rules v. Personal Data Protection Bill, 2019

NASSCOM®

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Definition expanded	Financial Data; Health data
Retained	Sexual Orientation; Biometric data
New Addition	Genetic data; Caste or tribe; Official Identifier; Religious or Political Belief or Affiliation; Transgender Status; Intersex Status; Sex life

Section 43A of the Information Technology Act, 2000 shall be omitted.

SPDI Rules v. Personal Data Protection Bill, 2019

NASSCOM®

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

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 PDPB, 2019, 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.**

Health data

The definition under PDPB, 2019, 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.**

Grounds for Processing Personal Data

NASSCOM®

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

- Data Principal's Consent
- Function of State
- Compliance with law or order of court/ tribunal
- Prompt action in case emergencies
- Purposes related to employment
- Reasonable Purpose of data fiduciary

Sensitive Personal Data can only be processed using explicit consent.

Data Principal Rights

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

Transparency and Accountability

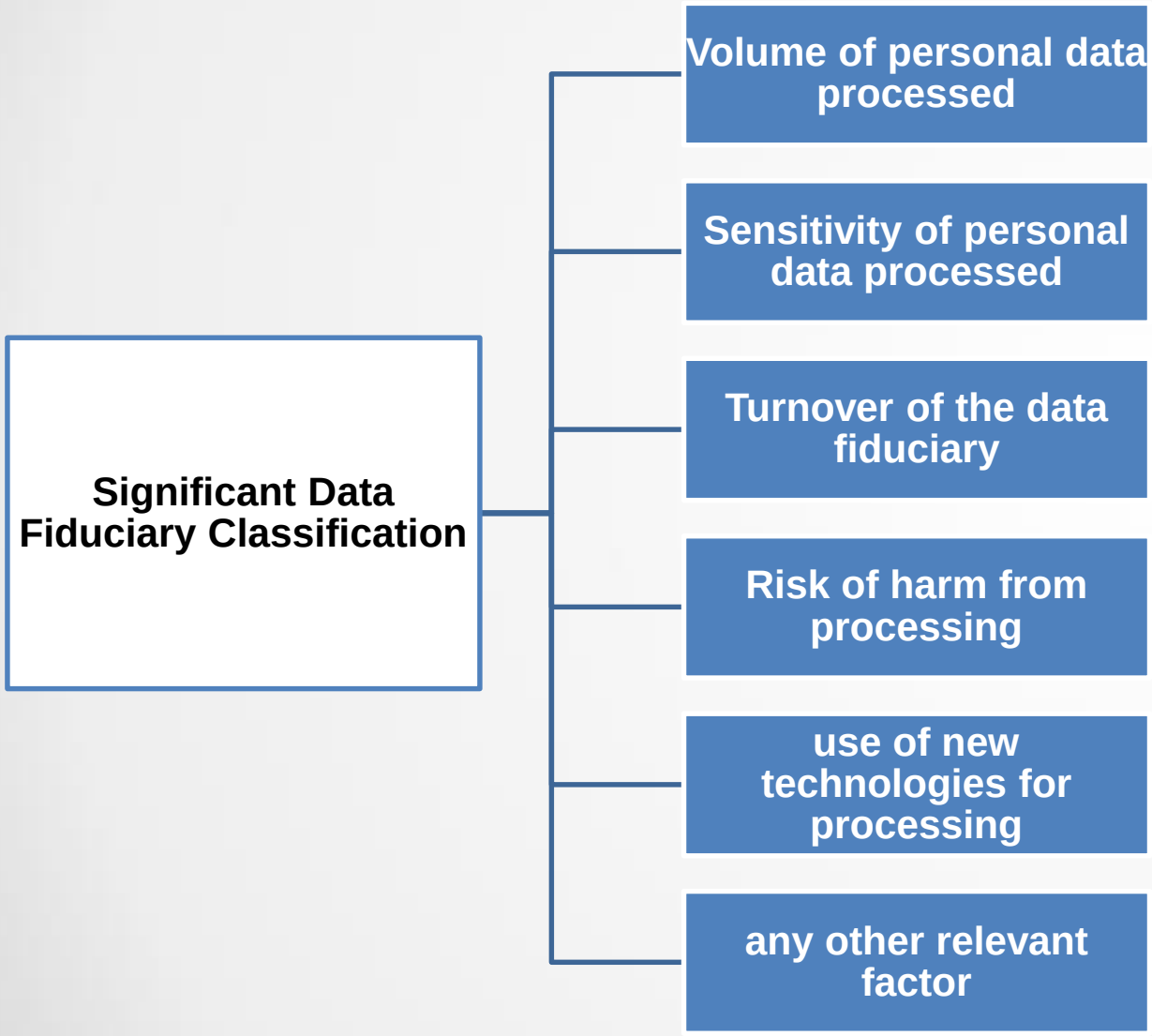
NASSCOM®

DSCI PROMOTING DATA PROTECTION

A NASSCOM® Initiative

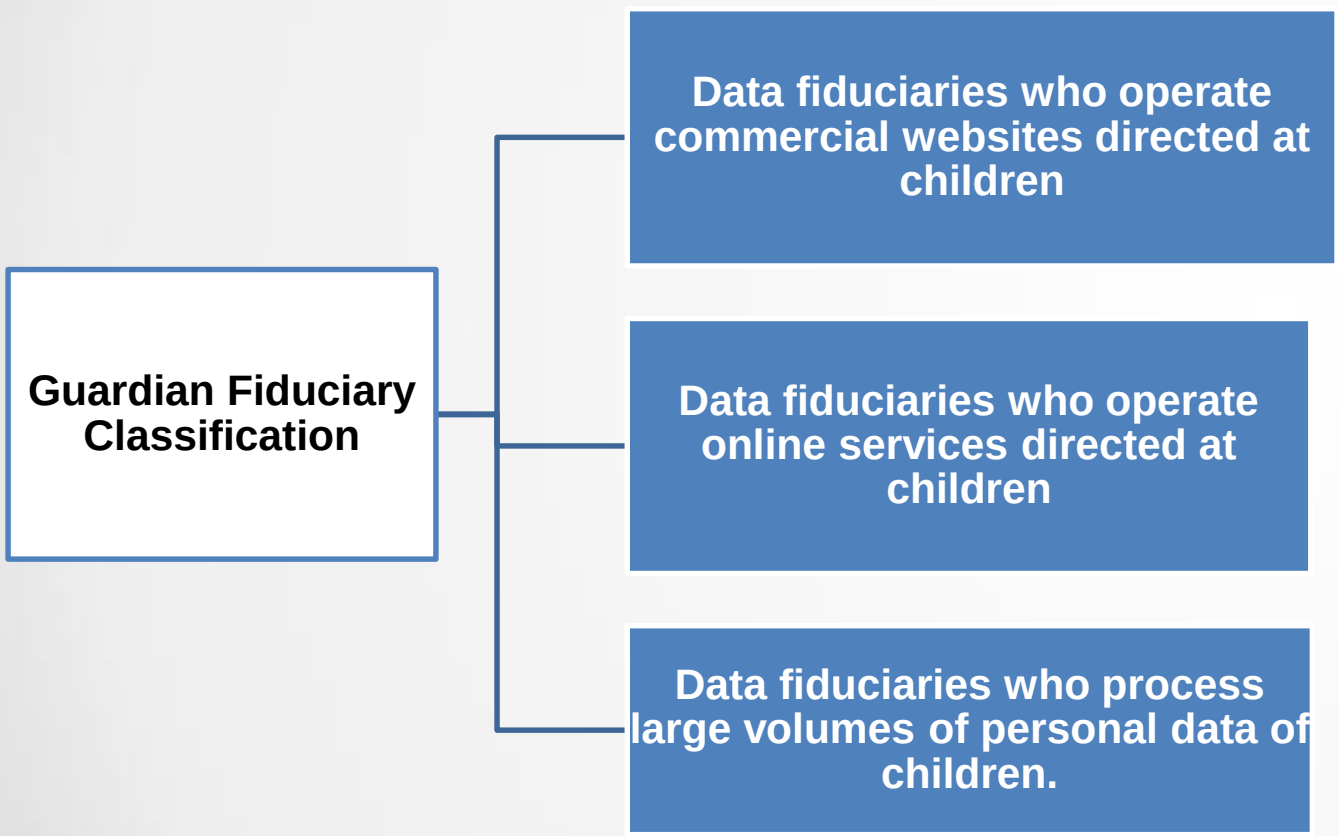
- Significant Data Fiduciaries
- Guardian Data Fiduciaries
- Privacy by Design Policy
- Data Audits
- Data Protection Impact Assessment
- Record Keeping
- Data Protection officer
- Grievance Redressal

Transparency and Accountability



Significant data fiduciaries obligations:
Conduct data protection impact assessments
Keep records of processing
subject to data audits
appoint data protection officer
subject to mandatory registration with the authority

Transparency and Accountability

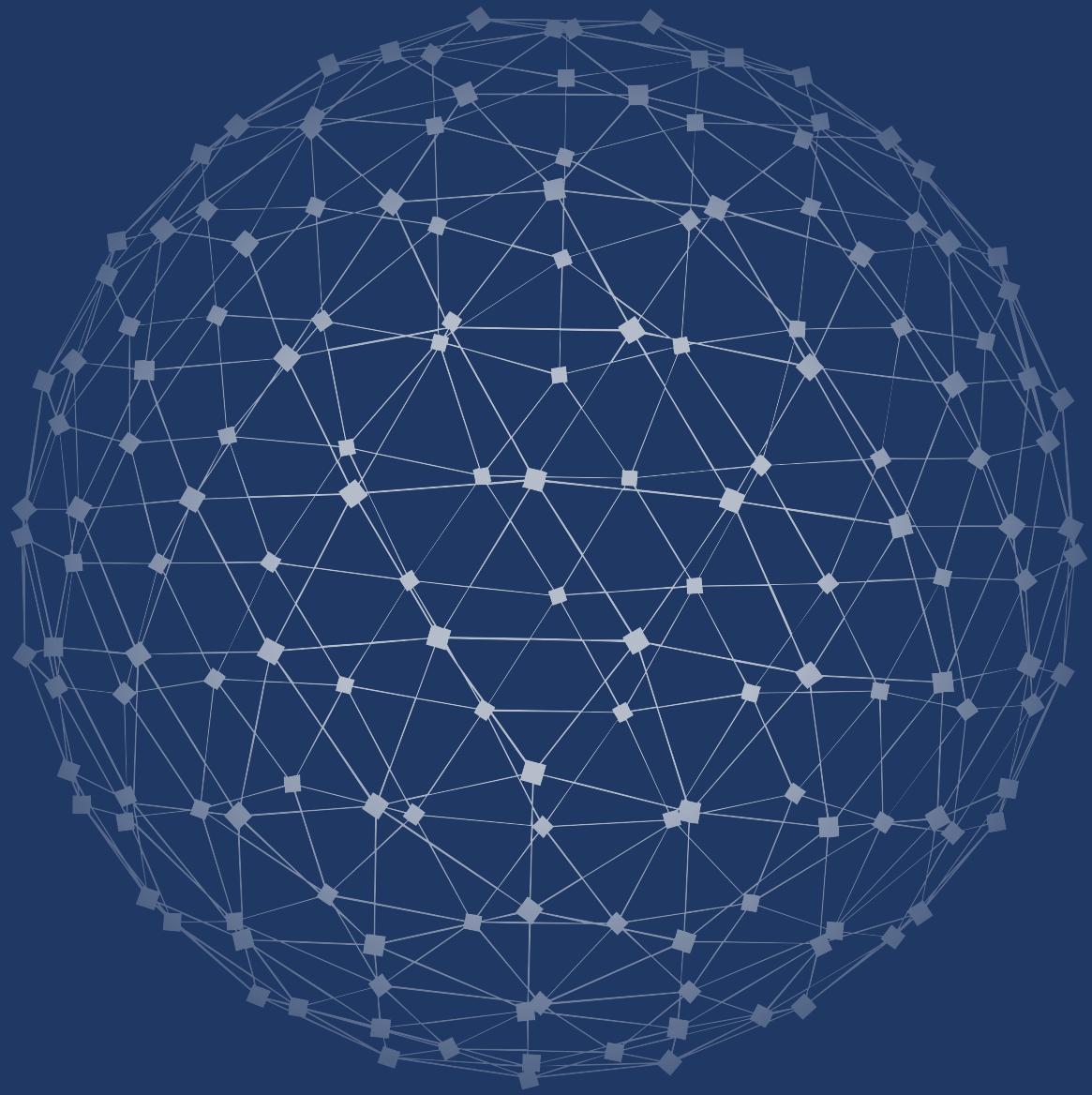


Guardian fiduciaries shall be barred from:
profiling, tracking, behavioural monitoring
targeted advertising directed at children
undertaking any other processing of personal data that can cause significant harm to the child

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

NASSCOM®

Key Changes



Personal Data

Personal Data Protection Bill, 2018	Personal Data Protection Bill, 2019	EU GDPR
“Personal data "means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information;	Definition of “personal data” has been amended to include data, “whether offline or online”, and “shall include any inference drawn from such data for the purpose of profiling” (Clause 3(28) of the PDP Bill)	‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Sensitive Personal Data

NASSCOM® DSCI PROMOTING DATA PROTECTION A NASSCOM® Initiative

Personal Data Protection Bill, 2018	Personal Data Protection Bill, 2019	EU GDPR
Passwords; financial data; health data; official identifier; sex life; sexual orientation; biometric data; genetic data; transgender status; intersex status; caste or tribe; religious or political belief or affiliation.	Definition of "sensitive personal data" has been amended to remove "passwords". The power to specify further categories of "sensitive personal data" has moved from the Authority to the Central Government, with a reference to Clause 15 of the PDP Bill. In arriving at this determination the Central Government will consult the DPA and the concerned sectoral regulator.	Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

NASSCOM-DSCI had recommend in its submission and has been continuingly advocating for the removal of financial data, official identifiers and passwords from the list of sensitive personal data.

Processing of Foreign Data

Personal Data Protection Bill, 2018	Personal Data Protection Bill, 2019	EU GDPR
Central government had the power of to exempt certain data processors dealing with personal data of data principals not within in the territory of India under S.104. The is provision was listed as a miscellaneous provision.	This provision has now been incorporated as an exemption; though the exemption is still subject to notification by the central government.	No such exemption is provided under EU GDPR.

NASSCOM-DSCI in its submission recommended that this power of central government to exempt certain data processors under S.104 should be reworded as an exemption and moved from Chapter XV (*Miscellaneous*) to Chapter IX (*Exemptions*).

Processing of Foreign Data

NASSCOM® DSCI PROMOTING DATA PROTECTION A NASSCOM® Initiative

NASSCOM-DSCI SUBMISSION:

i) 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 shall be exempt from the following provisions of the Act:

1. Restrictions on cross border transfer of personal data (Chapter VIII) (2) Conditions for cross border transfer of personal data (Chapter VIII)

ii) Further, the Central Government may, by notification, exempt the Processing of personal data of Data Principals mentioned in (i) above from the application of any provision of the Act, to the extent that the same is desirable to enable such processing to be in conformity with the requirements of the particular country where the:

1. Data Principals are located; or

2. Organization which alone or in conjunction with others determines the purpose and means of processing of personal data is located or incorporated.

Restrictions and Conditions Transfer of Personal Data Outside India

NASSCOM®

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Exempted Personal Data

(on ground of necessity or strategic interest of the state)

Personal Data

(a) Subject to standard contractual clauses or intra-group schemes; or
(b) Central Govt or DPA has permitted to a particular country; or
(c) a or b + consent

Sensitive Personal Data

a or b + explicit consent

Store a copy in data center/server in India

Critical Personal Data

Exceptions

- Health Services
- Emergency Services
- **Central Govt in consultation with DPA has permitted transfer to approved country**

Personal Data Protection Bill, 2018

Restrictions and Conditions Transfer of Personal Data Outside India

NASSCOM®

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Personal Data

Sensitive Personal Data

(a) Explicit consent + Subject to standard contractual clauses or intra-group schemes; or

(b) Explicit consent + Central Govt in consultation with DPA has permitted to a particular country; or

(c) Explicit consent + DPA has allowed transfer

Must also continue to be stored in India

Passwords excluded

Critical Personal Data

Exceptions

- Health Services
- Emergency Services
- **Central Govt in consultation with DPA has permitted transfer to approved country**

Personal Data Protection Bill, 2019

Significant Data Fiduciaries

Personal Data Protection Bill, 2018	Personal Data Protection Bill, 2019	EU GDPR
Significant data fiduciaries could be classified based on (a) volume of personal data processed; (b) sensitivity of personal data processed; (c) turnover of the data fiduciary; (d) risk of harm resulting from any processing or any kind of processing undertaken by the fiduciary; (e) use of new technologies for processing; and (f) any other factor relevant in causing harm to any data principal as a consequence of such processing.	Social media intermediaries have been added as a new class of data fiduciaries and can be classified as SDFs by the Central Government in consultation with the DPA. Social Media Intermediaries' would be required to enable voluntary self-verification by their users. Such users will have to be demarcated on the platform as being verified users. The manner and process of voluntary self-verification will be prescribed by the Central Government.	Classification of entities is limited to: a) Data Controller or Joint controller b) Data Processor c) Sub- Processor Only (a) and (b) are under the direct application of the law.

Transparency and Accountability Measures

Personal Data Protection Bill, 2018	Personal Data Protection Bill, 2019	EU GDPR
Measures that regulated entities under the bill must implement. These include: (a) Privacy by design, (b) data protection impact assessment, (c) record keeping, (d) appointing a data protection officer (e) data audits. Practices inscribed in (b) to (e) were to be carried about by data fiduciaries which can been classified as “significant data fiduciaries” by the Data Protection Authority.	Privacy by Design: The obligation for embedding privacy by design in operational and management practices has been simplified, and has been replaced with the requirement to put in place a privacy by design policy, which will have to be certified by the DPA and published on the website of the data fiduciary. Consent Managers: The Bill introduces the concept of data fiduciaries acting as consent managers.	(a) Privacy by design (b) data protection impact assessment (c) record keeping (d) appointing a data protection officer

Non Personal Data

Personal Data Protection Bill, 2018	Personal Data Protection Bill, 2019	EU GDPR
The bill did not cover Annoymised data as part of its scope of application.	The bill doesn't apply to Annoymised data with respect to obligations and compliance requirements laid out in the bill. [clause 2(3)] However, the central government is empowerment to create polices to direct data fiduciaries or data processors to share Annoymised data or non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the central government. [clause 91]	Annoymised data is out of the scope of application.

Exemptions

Personal Data Protection Bill, 2018	Personal Data Protection Bill, 2019
Exemption on the ground of security of the state limited to: (a) Chapter II, except section 4; (b) Chapter III; (c) Chapter IV; (d) Chapter V; (e) Chapter VI; (f) Chapter VII, except section 31; and (g) Chapter VIII of the bill.	The exemption on the ground of security of the state has been expanded (Clause 35 of the PDP Bill: • The Article 19(2) grounds have been referenced • The scope of the exemption has been extended to any agency of the Government with regard to any or all of the provisions of the Act. Sandbox for encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest. Exempted provisions: (i) the obligation to specify clear and specific purposes under sections 4 and 5; (ii) limitation on collection of personal data under section 6; (iii) any other obligation to the extent, it is directly depending on the obligations under sections 5 and 6; and (iv) the restriction on retention of personal data under section

Compensation, Penalties and Offences

Personal Data Protection Bill, 2018	Personal Data Protection Bill, 2019	EU GDPR
Penalties: (a) Five crore rupees or two per cent of total worldwide turnover (b) 15 crore rupees or 4 percent of total worldwide turnover Compensation: No bar on the monetary value of the compensation. Offences: a) Obtaining, transferring or selling of personal data contrary to the b) Obtaining, transferring or selling of sensitive personal data contrary to the Act c) Re-identification and processing of de-identified personal data d) Offences by companies	Penalties and compensation provisions remain unchanged in terms of quantum. Offences: a) Re-identification and processing of de-identified personal data b) Offences by companies	Penalties: a) Up to €10 million, or 2% of annual global turnover b) Up to €20 million, or 4% of annual global turnover Compensation: No bar on the monetary value of the compensation. Offences: No such provisions

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

NASSCOM®

Thank you!

Share your inputs with us on: anand.Krishnan@dsci.in or indrajeet.@nasscom.in