Overview of The Digital Personal Data Protection Bill, 2022*

CS Ranganath Khanolkar
27 May 2023

*Based on the draft bill published by the Ministry of Electronics and Information Technology on 7 December 2022

The Digital Personal Data Protection Bill, 2022
Is it relevant for a CS?

- No exemptions for professional firms/ small businesses
- Processing of personal data in digital form is unavoidable
- Massive financial penalties for non-compliance (Max. INR500Crs)
- Career opportunities as a Data Protection Officer (of Significant Data Fiduciaries)

The Digital Personal Data Protection Bill, 2022
Agenda

1. Need for a law
2. Global scenario and adequacy
3. Journey of the bill
4. Key concepts
5. Applicability
6. Compliance requirements
7. Enforcement & penalties
8. Next steps & closing thoughts

The Digital Personal Data Protection Bill, 2022
Need for a Law

▪Art. 21 of the Constitution (fundamental right to life and liberty of citizens)

▪The Information Technology Act, 2000 & Sensitive Personal Data Rules, 2011

▪Sectoral laws (e.g. DND/ NCPR Regulations)

- Limited privacy protections available under a patchwork of laws
- Heightened risk of personal data misuse
- No individual rights
- Enabling seamless international data flows/ achieving "adequacy"

The Digital Personal Data Protection Bill, 2022
Global Scenario and Adequacy

DLA Piper Global Data Protection Laws of the World - World Map (dlapiperdataprotection.com)

Gold standard of privacy laws

- The General Data Protection Law (GDPR): European Union
- Argentina, Japan, South Africa, South Korea, Switzerland, United Kingdom all have GDPR-type legislation

→

Restrictions on data flows (i.e. some form of data localisation/ residency requirements)

→

No restrictions on data flows to whitelisted countries ("adequate jurisdiction")

Bill aims to support India's effort to achieve the tag of "adequate jurisdiction"

The Digital Personal Data Protection Bill, 2022
Journey of the bill

2010-2012

2010: Approach paper on Legal Framework for Privacy

2012: Expert Committee report recommended privacy legislation in India

2017

July 31: Govt. sets up Justice Srikrishna Committee

August 24: SC holds privacy as fundamental right (Puttaswamy Case)

November 27: Justice Srikrishna Committee seeks comments on White Paper on data protection framework in India

2018-2019

July 26, 2018: Justice Srikrishna Committee submits report and a draft bill (v1)

August 14, 2018: Govt. seeks comments on draft bill

December 11, 2019: Personal Data Protection Bill, 2019 introduced in the Lok Sabha which was referred to Joint Parliamentary Committee (JPC) (v2)

2020-2022

8 December 2021: JPC submitted their report along with a revised draft of the bill after extensive consultations (v3)

3 August 2022: Bill withdrawn considering the numerous changes suggested by JPC

7 December 2022 – Fresh bill released for public feedback (v4)

Amended bill expected to be tabled in monsoon session (v5)

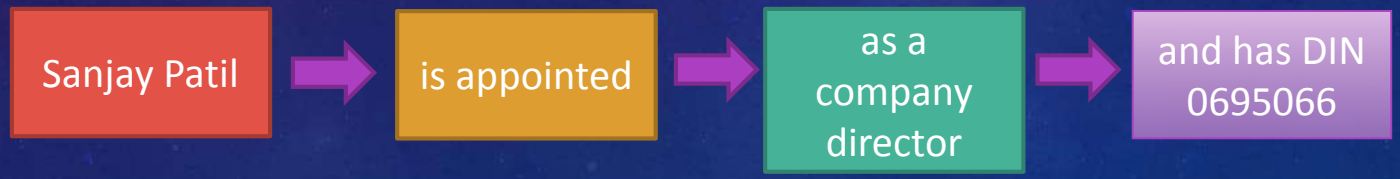
The Digital Personal Data Protection Bill, 2022
Key Concepts

"**Data**" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means [Section 2(4)].

"Personal Data" means any data about an individual who is **identifiable** by or in relation to such data [Section 2(13)].

Identifiable and not "identified".

- Ambiguity about identifiability
- GDPR:
  - Possibility of identification itself is sufficient to treat the data as personal data (even though it may be difficult to identify the individual)
  - Related data need not be true or accurate



The Digital Personal Data Protection Bill, 2022
Key Concepts
Is this personal data?

Category (Assumption: No other accompanying information)	Yes	No	Could be
First name		√	
Last name		√	
Full name			√
Personal email-ID	√		
Business email-ID	√		
Home address	√		
Office address		√	
Bank account number	√		
Blood group		√	
Telephone No.	√		
CIN No		√	

The Digital Personal Data Protection Bill, 2022
Key Concepts

Is this personal data?

Category (Assumption: No other accompanying information)	Yes	No	Could be
CCTV footage at a restaurant	√		
Total No. of orders placed on a website (aggregated data)		√	
Photograph			√
Medical records	√		
Vehicle registration No.	√		
Pseudonymized data	√		
Anonymized data		√	
IP address	√		
Website cookies			√

The Digital Personal Data Protection Bill, 2022
Key Concepts

“Processing” in relation to personal data means an automated operation or set of operations performed on digital personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction [Section 2(16)]

“Data Principal” means the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child [Section 2(6)]

"personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data. [Section 2(14)]

The Digital Personal Data Protection Bill, 2022
Key Concepts

"Data Fiduciary" means ***any person*** ***who alone or in conjunction with other persons*** ***determines the purpose and means of processing of personal data*** [Section 2(5)]

In relation to this program, who is the data fiduciary?

Purpose: The Why?

- To create a record of attendance
- To issue CPE hours
- To send you payment receipt
- To contact you for updates regarding the program

Means: The How?

- modes of registration
- Payment options
- Place of storage
- Medium for sending updates

Data Fiduciary responsible for most of the compliances and also liable for non-compliance by data processors

Data Processor" means any person who processes personal data on behalf of a Data Fiduciary;

The Digital Personal Data Protection Bill, 2022
Key Concepts

Transaction/ Scenario of Company - ABC Pvt Ltd	Data Principal	Data Fiduciary	Data Processor
Company advertises a job position on a job portal?	Candidates/ Prospective employees	Company	Job portal
Company runs a mass email campaign for promoting its new products to its B2C clients	Clients	Company	Email service provider
Company runs a mass email campaign for promoting its new products to its B2B clients	Employees/ officers of clients	Company	Email Service Provider
Company shares payroll data with a payroll service provider	Employees of the company	Company	Payroll Service Provider
Company purchases a database of leads/ prospects from a data broker/ aggregator	Clients/ Employee of clients	Both the company and the data-broker	
Company shares compensation data with their auditors	Employees of the company	Both the company and the auditor	
Company organises a co-branded webinar with another company	Webinar attendees	Both companies	Webinar hosting provider

The Digital Personal Data Protection Bill, 2022 Applicability

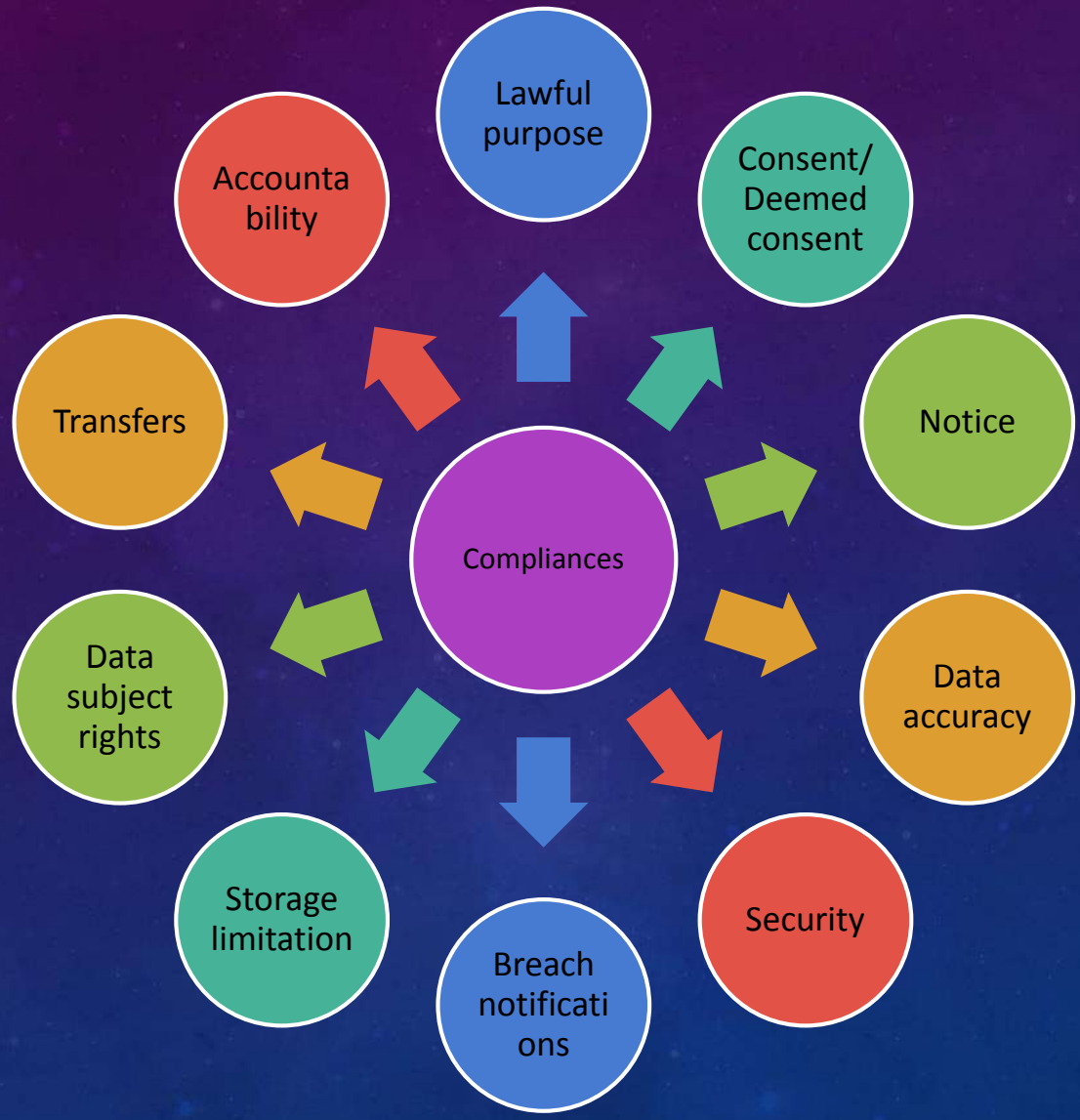
Bill has extraterritorial application [Sections 4(1) and 4(2)]

Processing	Data Fiduciary Location		Data Principal Location	
	In India	Outside India	In India	Outside India
Within India	Applicable		Applicable	Applicable (unless exempted by Govt. by notification)
Outside India	Applicable (if in connection with profiling or offering of goods to data principals within India)		Applicable	Not Applicable

The Digital Personal Data Protection Bill, 2022
Applicability

Does not apply to [Section 4(3)]:	Non-automated processing of personal data
	Offline processing
	Processing for domestic or personal purpose
	Processing of personal data contained in a record which is > 100 years old

The Digital Personal Data Protection Bill, 2022 Compliance Requirements



Security and Breach Notifications apply to data processors also

The Digital Personal Data Protection Bill, 2022 Compliance Requirements – Grounds of Processing

LAWFUL PURPOSE [SECTION 5]

Processing should be for a lawful purpose (i.e. for a purpose that is not forbidden by law) [Section 5]

CONSENT/ DEEMED CONSENT [SECTION 5 and 7]

Processing should based on Consent Or Deemed Consent of the Data Principal

Requirements of a valid Consent:

- Freely given : Meeting of minds
- Specific: For a specific purpose
- Informed: Information about the purposes as well as all relevant aspects of the processing
- Unambiguous indication of data principal's wishes: No pre-ticked boxes, small fonts
- Should be in plain and clear language [English or any language stated in the 8th Schedule of the Constitution]
- Capable of being withdrawn: Ease of withdrawal should be comparable to the ease of giving consent

The Digital Personal Data Protection Bill, 2022 Compliance Requirements – Grounds of Processing

Download the Latest Amendments on Company Law from M/s ABC & Associates

Name* _____

Email Address * : _____

Company Name * : _____

DOWNLOAD

✕

Download the Latest Amendments on Company Law From M/s ABC & Associates

Name * _____

Email Address * : _____

Company Name * : _____

DOWNLOAD

☐ I agree to be contacted by M/s ABC & Associates for providing information about their services

☐ I agree to be receive monthly updates on company laws

Please refer to our privacy policy for further information

✔

The Digital Personal Data Protection Bill, 2022 Compliance Requirements – Grounds of Processing

Deemed Consent [Section 8]

Consent is deemed when processing is necessary:

- In situation where the data principal voluntarily provides personal data and it is reasonably expected that the data principal would provide such personal data
- For the performance of function under any law, or provision of service or benefit to the data principal, or the issuance of any certificate, license or permit for any action or activity of the Data Principal, by the State or any instrumentality of the State
- For compliance with any judgment or order issued under law;
- For responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;
- for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health
- for taking measures to ensure safety of, or provide assistance or services to any individual during any disaster, or any breakdown of public order;
- for the purposes related to employment, including prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, recruitment, termination of employment, provision of any service or benefit sought by a Data Principal who is an employee, verification of attendance and assessment of performance;
- in public interest, including for: (a) prevention and detection of fraud; (b) mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws; (c) network and information security; (d) credit scoring; (e) operation of search engines for processing of publicly available personal data; (f) processing of publicly available personal data; and (g) recovery of debt;
- for any fair and reasonable purpose as may be prescribed

The Digital Personal Data Protection Bill, 2022 Compliance Requirements – Notice [Section 6]

- To be provided to data principal
- On or before requesting for consent
- Needs to be itemised
- In clear and plan language [English or any language specified in the 8th Schedule to the Constitution]
- Containing description of personal data sought to be collected and purpose of processing
- Can be a separate document (e.g. a privacy notice)

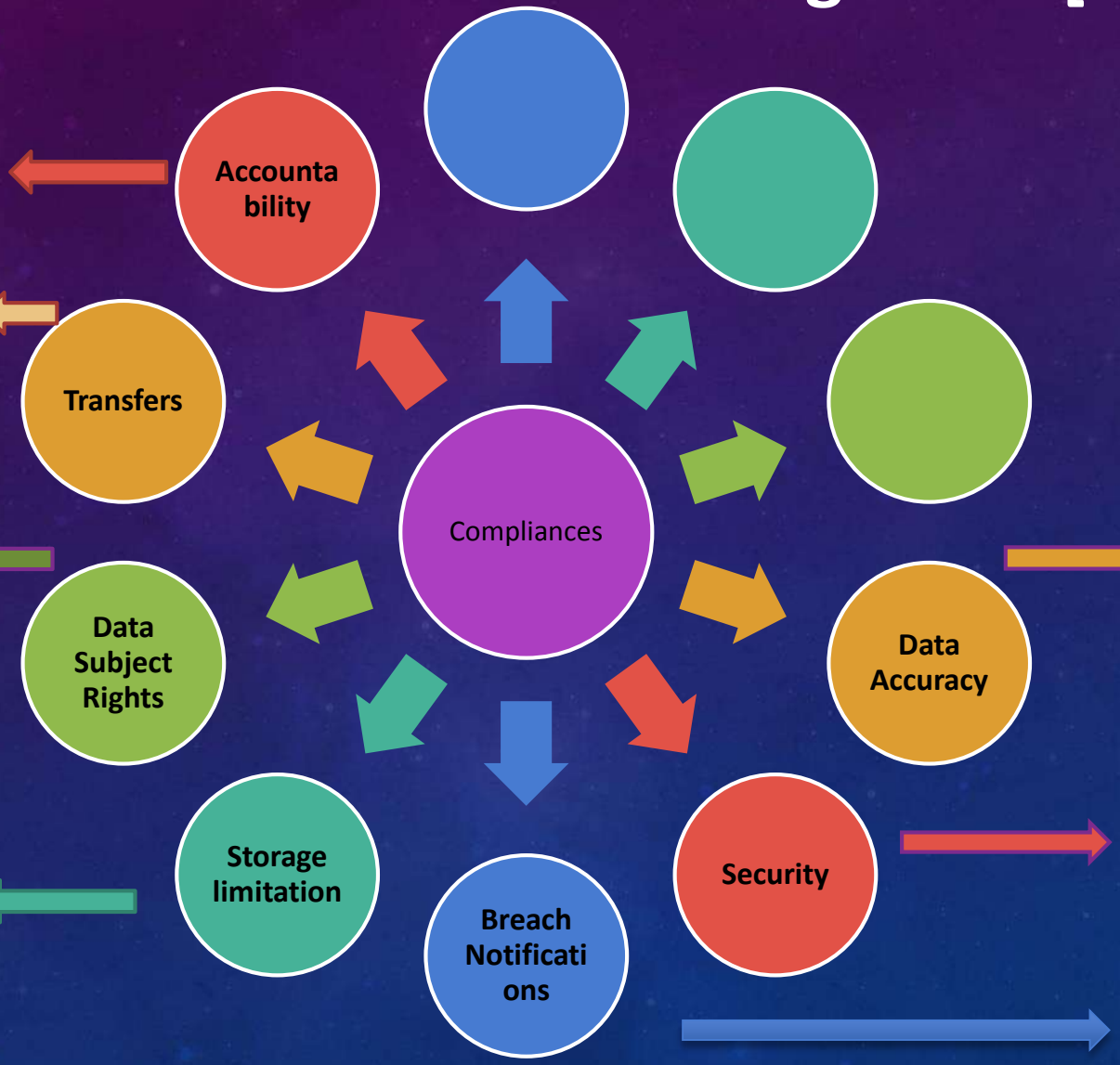
The Digital Personal Data Protection Bill, 2022
Compliance Requirements – General obligations [Section 9]

Fiduciary responsible/ liable for compliance by processors. Sharing of personal data with other fiduciaries or processors only under a valid contract

Transfers of personal data only to whitelisted countries, subject to prescribed rules

Right to (a) information; (b) correction and erasure; (c) grievance redressal; (d) nominate

Cease to retain personal data or anonymize it after purposes of collection have been served and retention is no longer necessary for legal and business purpose. Also require data processors to cease/ anonymize



Fiduciary to ensure personal data remains accurate and complete if : (a) its likely to be used to make decision that affects the data principal; or (b) likely to be disclosed to another data fiduciary

(a) Implement effective technical & organisational measures
(a) Take reasonable security safeguards to prevent personal data breach

Notify data protection board and affected data principal in the event of personal data breach

The Digital Personal Data Protection Bill, 2022
Compliance Requirements – Data Subject Rights [S 12 -15]

Information

- Confirmation whether fiduciary is processing or has processed personal data
- Summary of personal data being or that has been processed and the related processing activities
- Identities of other data fiduciaries with whom data is shared
- Any other information as prescribed

Correction and erasure

- Correction of inaccurate or misleading data
- Complete incomplete personal data
- Update personal data
- Erase personal data that is no longer necessary for the purposes for which it was processed, unless retention is necessary for a legal purpose

Grievance Redressal

- Register grievance
- In case not satisfied with response or no response within 7 days, then complaint to the data protection board

Nominate

- In the event of death or incapacity

The Digital Personal Data Protection Bill, 2022
Compliance Requirements – Additional Obligations [S 10-11]

Processing of personal data of children

- Need to obtain verifiable parental/ guardian consent
- Not to undertake processing that is likely to harm the child
- Not undertake tracking or behavioural monitoring of children or targeted advertising directed at children

Significant Data Fiduciary

- Central Govt may notify any data fiduciary or class of data fiduciary as a Significant Data Fiduciary based on certain factors
- Significant data fiduciary to appoint a Data Protection Officer (DPO), reporting to the Board of Directors or similar body. DPO to be the point of contact for grievance redressal
- Significant data fiduciary to appoint a data auditor to evaluate compliance
- Conduct a data protection impact assessment in relation to the processing.

The Digital Personal Data Protection Bill, 2022 Compliance Requirements – Exemptions [S 18]

General

- Processing necessary for enforcing a legal right or claim
- Processing necessary for performance of a judicial or quasi-judicial function
- Processing in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law
- Data principals not within India and processing is under a contract with any person outside of India (outsourcing exemption)

Government/ State

- Central Government may by notification exempt processing by any instrumentality of the State in the interest of sovereignty and integrity of India, friendly relations with foreign states, maintenance of public order or preventing incitement to any cognizable offence
- Central Government may by notification exempt processing necessary for research, archiving or statistical purpose if personal data is not to be used to take any decision specific to data principal and subject to certain standards to be set by the data protection board
- Central Government may by notification exempt certain compliances for certain data fiduciaries or class of data fiduciaries
- Security requirements do not apply to processing by the State or any instrumentality of the State

The Digital Personal Data Protection Bill, 2022
Enforcement and Penalties [Sections 19 – 25]

Schedule 1

(See section 25)

Sl. No.	Subject matter of the non-compliance	Penalty
(1)	(2)	(3)
1	Failure of Data Processor or Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (4) of section 9 of this Act	Penalty up to Rs 250 crore
2	Failure to notify the Board and affected Data Principals in the event of a personal data breach, under sub-section (5) of section 9 of this Act	Penalty up to Rs 200 crore
3	Non-fulfilment of additional obligations in relation to Children; under section 10 of this Act	
4	Non-fulfilment of additional obligations of Significant Data Fiduciary; under section 11 of this Act	Penalty up to Rs 150 crore
5	Non-compliance with section 16 of this Act	Penalty up to Rs 10 thousand
6	Non-compliance with provisions of this Act other than those listed in (1) to (5) and any Rule made thereunder	Penalty up to Rs 50 crore

The Digital Personal Data Protection Bill, 2022 Enforcement and Penalties [Sections 19 – 25]

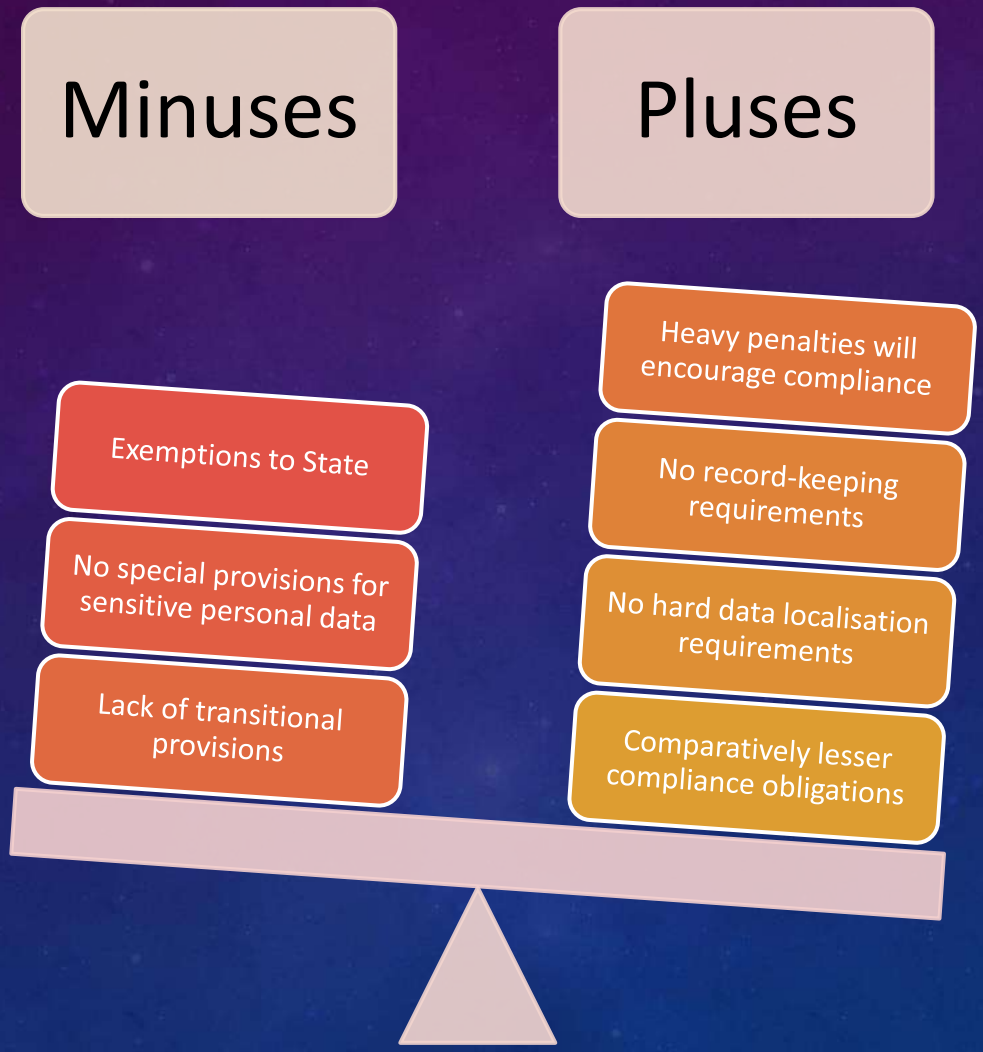
Data Protection Board of India (DPBI)

- Consisting of Chairperson, Members, Chief Executive Officer
- Powers of Civil Court as provided under CPC
- Functions
  - Determine non-compliance and impose penalties
  - Perform functions assigned by Central Govt
- Power to issue directions to any person for performance of its functions and may modify, withdraw, suspend cancel such directions
- Power to direct a data fiduciary to adopt urgent measures in case of a personal data breach
- Power to accept voluntary undertakings in lieu of further proceedings
- Power to review its own orders
- Appeals lie to High Court

The Digital Personal Data Protection Bill, 2022
Next Steps & Closing Thoughts

- Structure a privacy team
- Data Inventory/ Mapping
- Determine the different processing activities
- Review grounds of processing
- Information security policies
- Data processing contracts
- Design processes for data subject rights

The Digital Personal Data Protection Bill, 2022
Next Steps & Closing Thoughts



The Digital Personal Data Protection Bill, 2022
Q&A