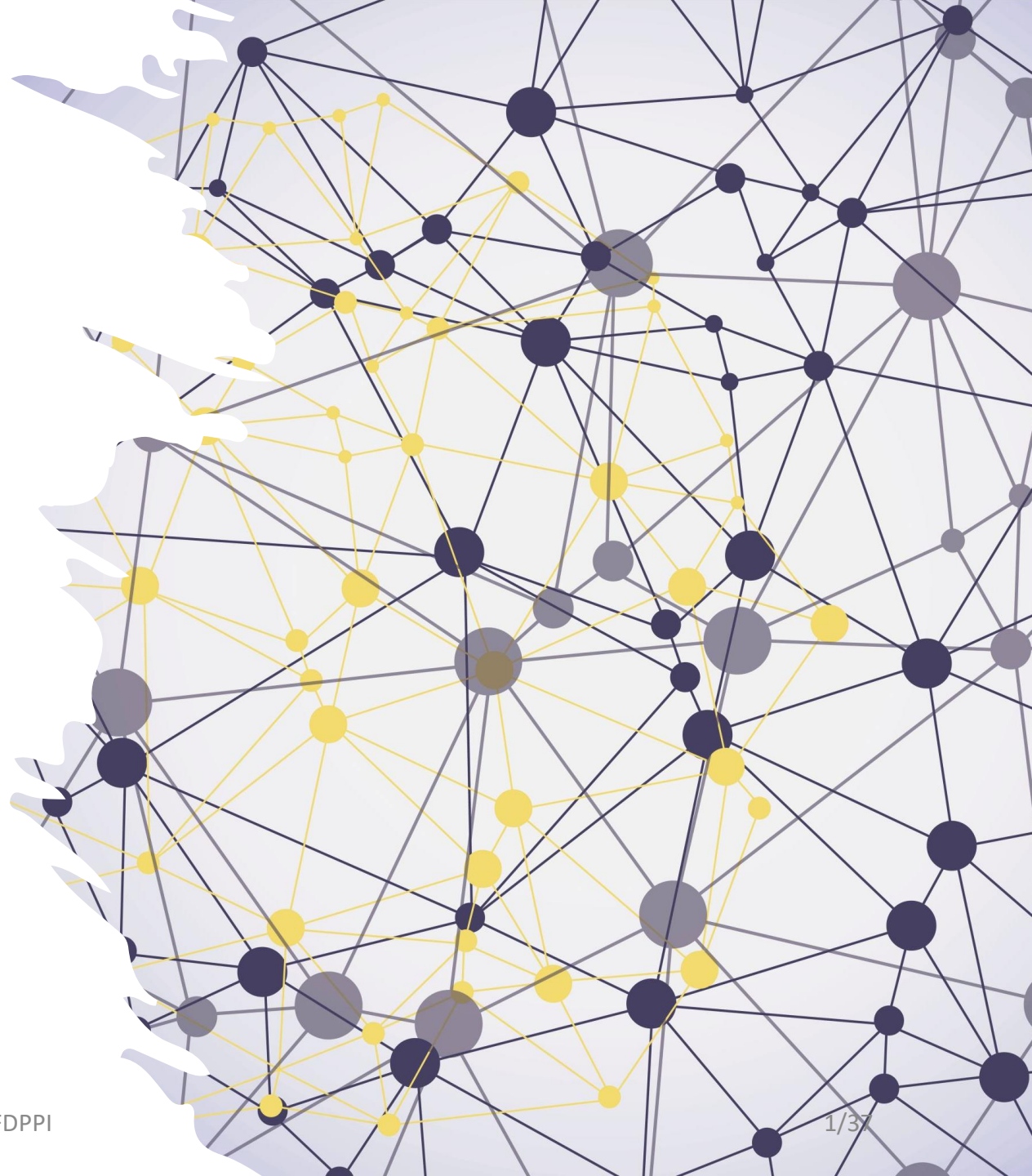
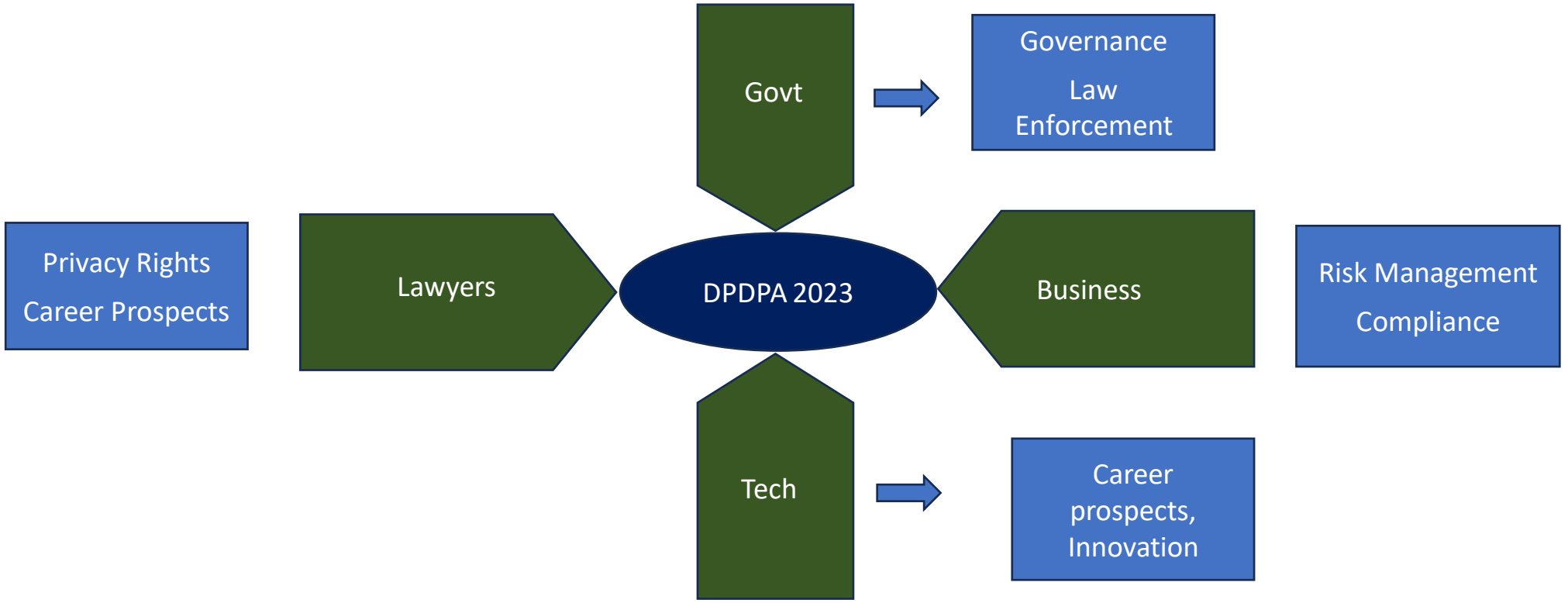
Compliance Requirements under DPDPA 2023

Naavi

(Nalsar_26/2/2024)



Different Perspectives



Naavi/FDPPI 2/24

Legal Perspective

- DPDPA 2023 was gazette notified on 11th August 2023. Rules not yet notified.
- **Is DPDPA 2023 is effective today?**
  - Could be a debatable issue
- DPDPA is called Digital Personal Data Protection Act
  - **Why it is not called a "Privacy Protection Act"?**
- What is the relationship of DPDPA 2023 with
  - **ITA 2000?**
  - Digital Evidence provisions in the New IEA?
- What will be the **role of CERT In** as a regulator after DPB comes into existence?
- What is the **Grievance Redressal Mechanism**
- What is **Nomination** of Personal Data?
- What are the **rights** and obligations of Data Principals
- What are the **consequences** of infringement and remedies to individuals?

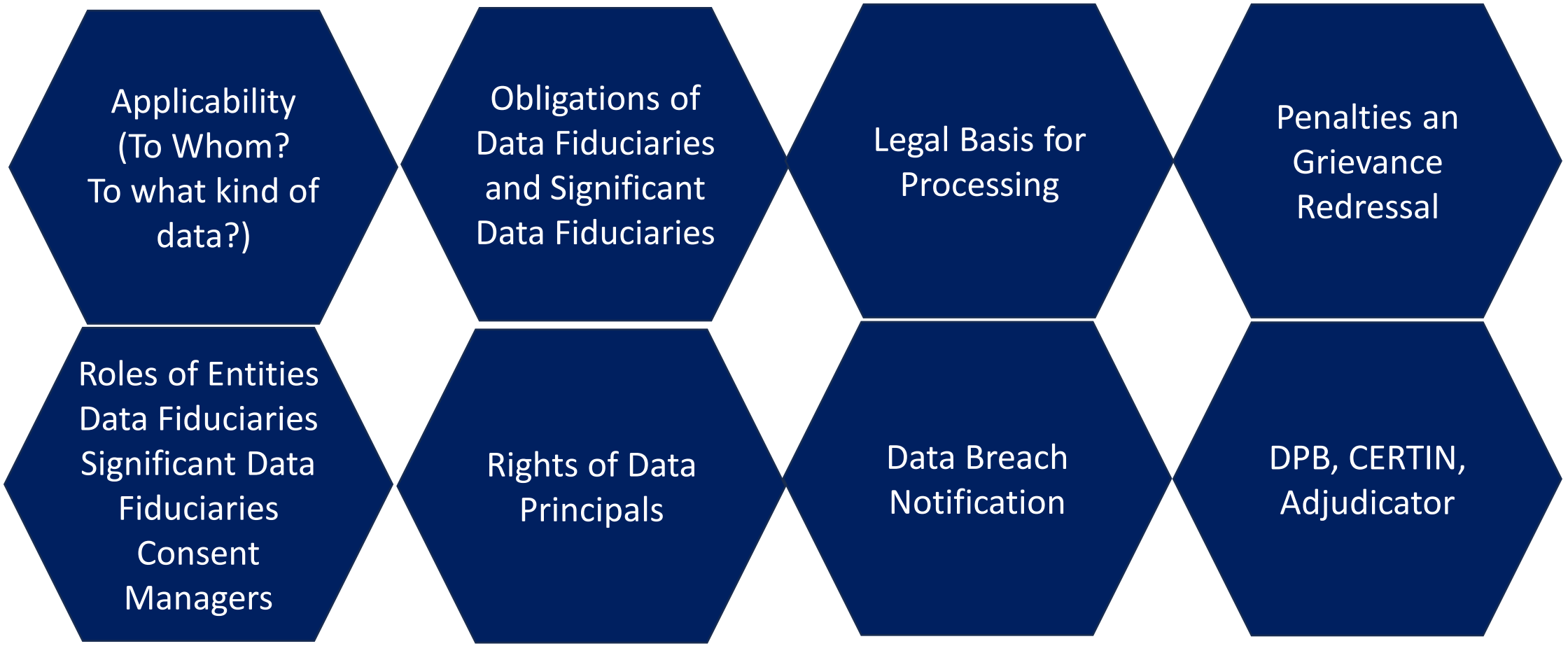
Government Perspective

- What are the exemptions available?
  - For Governance
  - For Law Enforcement
  - For National Security

Tech/Business Perspective

- What are the obligations for an organization?
  - Principles of processing, Mandatory requirements of appointing a DPO or conducting a Data Audit or Reporting a Data Breach etc
- Who is a Data Fiduciary and who is a Data Processor
- Who is a Significant Data Fiduciary
- Who is a consent Manager
- What are the penalties
- Special Exemptions if any to different sectors

Essence of DPDPA 2023



Penalties

S No	Subject Matter of Breach	Penalty
1	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach, under sub-section (5) of section 8	May extend to two hundred and fifty crore rupees.
2	Breach in observing the obligation to give the Board or affected Data Principals notice of a personal data breach, under sub-section (6) of section 8	May extend to two hundred crore rupees.
3	Breach in observance of additional obligations in relation to children, under section 9	May extend to two hundred crore rupees.
4	Breach in observance of additional obligations of Significant Data Fiduciary, under section 10	May extend to one hundred and fifty crore rupees.
5	Breach in observance of the duties under section 15	May extend to ten thousand rupees.
6	Breach of any term of voluntary undertaking accepted by the Board under section 32	Up to the extent applicable for the breach in respect of which the proceedings under section 28 were instituted.
7	Breach of any other provisions of this Act, other than the provisions of section 16	May extend to fifty crore rupees.

Penalties under ITA 2000

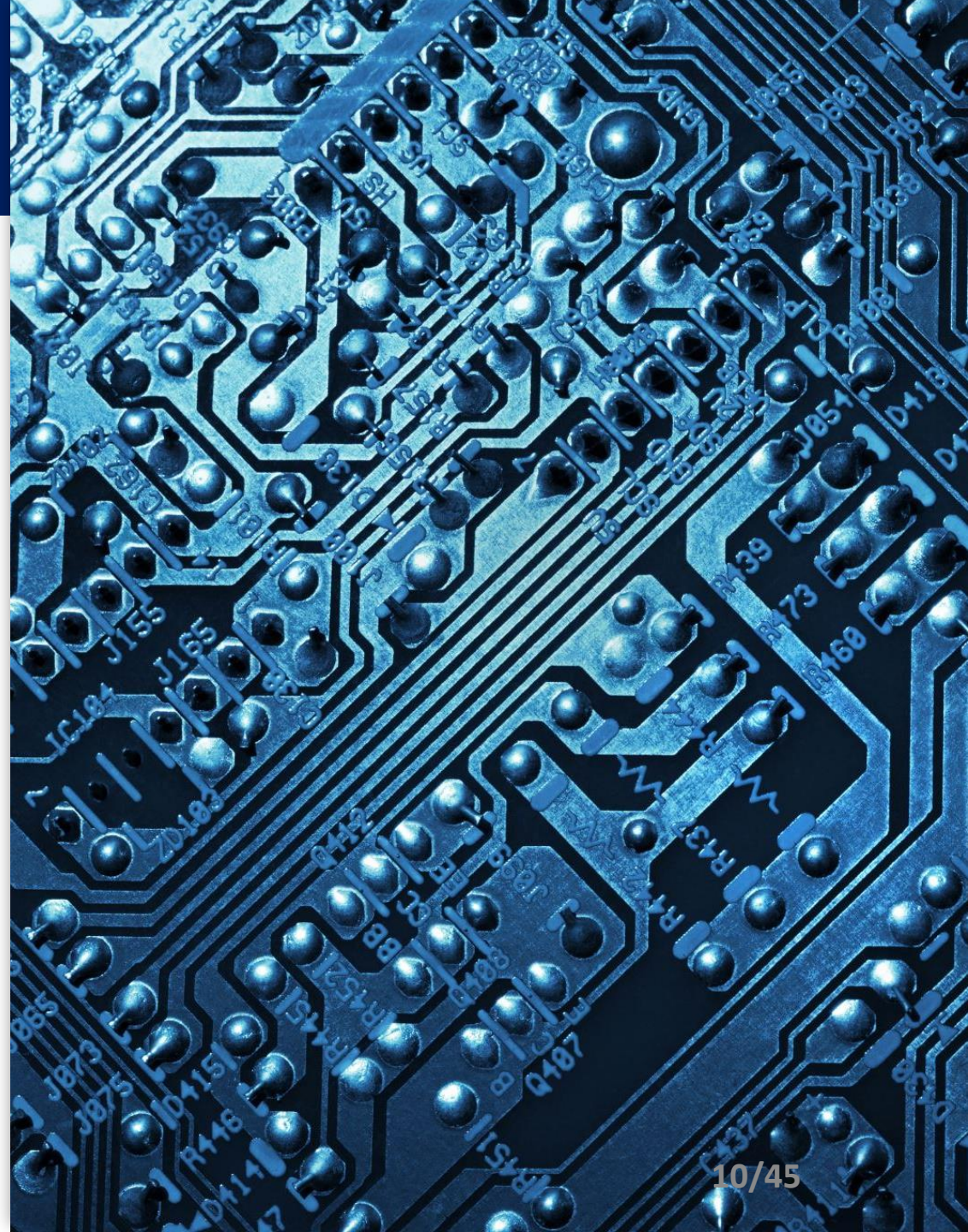
- Every data breach of personal data is a potential Section 43 contravention of ITA 2000 and Section 66 offence of ITA 2000
- Additionally, violations of CERT In Guidelines, violation of Section 67C/65, Section 72A, Section 1(4), 66C,66D, 66F etc may become relevant
  - Data Processors may also be “Intermediaries” under ITA 2000
  - With Section 85 liabilities on the companies may apply to executives
  - Section 43A requires “Due Diligence” and DPDPA 2023 itself is the due diligence under ITA 2000.
  - Hence criminal penalties under ITA 2000 may be relevant to Data Fiduciaries and Data Processors.
- Data Principals may invoke adjudication under Section 46 of ITA 2000 claiming for personal remedy for DPDPA 2023 non compliance

Corporate Objective: Compliance by Design

- To mitigate the Penalty Risk under DPDPA 2023 and ITA 2000
- How?
  - Is it by Privacy by Design? Or
  - Is it by Compliance by design?
- What is compliance by design?
  - Set up a Data Governance and Protection Management System (DGPMS) which is "by default" compliant with
    - DPDPA 2023 and ITA 2000
    - To mitigate the risk of administrative penalties under DPDPA 2023 and compensation claims under ITA 2000
      - Over and above the possible damages arising out of GDPR

Structure of DGPMS

- According to DPDPA 2023, A Data Fiduciary shall implement appropriate technical and organisational measures to ensure **effective observance of the provisions** of this Act and the rules made thereunder.
- DGPMS (Data Governance and Protection Management System) is the aggregation of Hardware, Software, People and Processes that are necessary for compliance of DPDPA 2023 as applicable.



Nature of DPDPA 2023 compliance

- DPDPA 2023 compliance is a Legal Compliance in a Technology environment
  - It is not amenable for complete automation.
  - Automation is only a tool to be used by a responsible compliance official
  - Hence human intervention in compliance is essential.
- Can AI take the full responsibility?
  - AI can take responsibility for part of the implementation routine.
  - But unless AI is sentient, it cannot replace the humans in the DPDPA 2023 compliance framework.

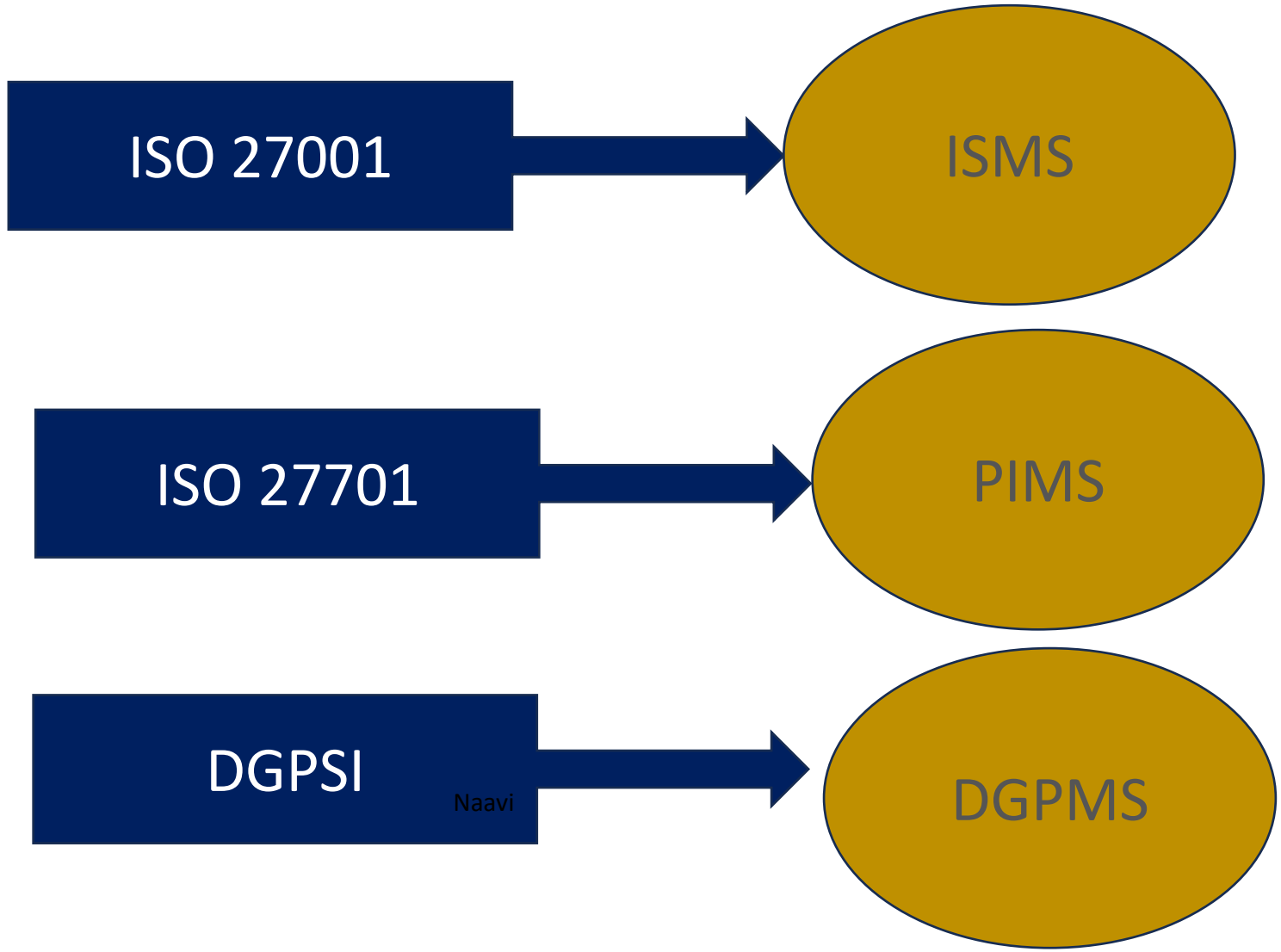
Reference Framework

- At present, the only reference framework for compliance for DPDPA 2023 compliance is
  - DGPSI or Digital Governance and Protection Standard of India which addresses
    - DPDPA 2023
    - ITA 2000
    - BIS standard (Draft) for Data Governance which includes Data Protection
  - Developed and implemented by FDPPI, a Section 8 Company of Data Protection Professionals in India.
- ISO 27001 addresses only the CIA aspect of information Security
- ISO 27701 addresses GDPR requirements

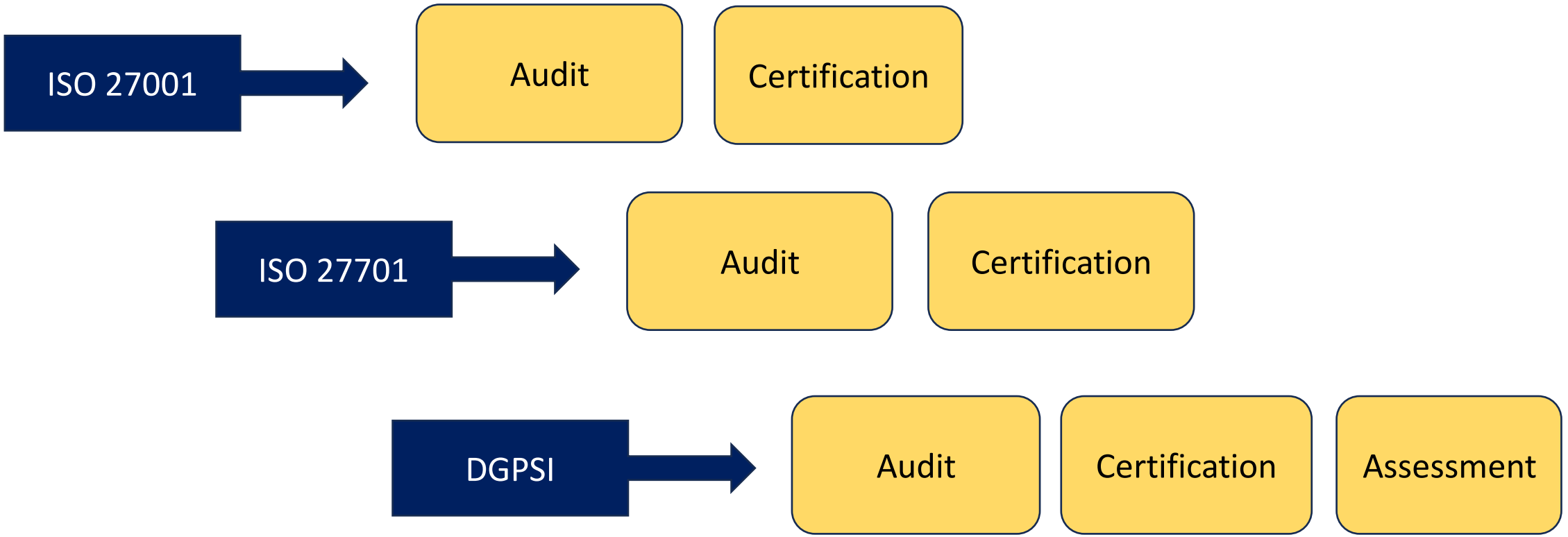
DGPSI Lite	DGPSI-Full
For DPDPA 2023 compliance without frills	For DPDPA 2023 compliance along with ITA 2000 and BIS standard for Data Governance to the extent applicable for personal data.
36 Model Implementation Specifications (MIS)	50 Model Implementation Specifications (MIS)

Two Versions of DGPSI

DGPMS is the system created by DGPSI



DGPSI is a system For Audit and Assessment



Naavi

15/37

Reduction of Compliance burden

- ISO 27701 compliance requires
  - 93 controls of ISO 27001
  - 49 controls of ISO 27701
- ITA 2000 compliance requires 33 controls (under IISF 309)
- BIS DGDMS compliance of G-7 (Data Privacy risks) requires 25 goals
  - Total 200 controls
- DPDPA 2023 requires 36 Implementation guidelines under DGPSI-Lite and 50 Implementation guidelines under DGPSI full
  - A substantial reduction of the compliance burden

DPDPA Compliance List-1: DGPSI-Lite

1	Sec 4	4.1	Establish whether the organization is **processing personal data for a lawful purpose** to which DPDPA is applicable and whether the organization is determining the Purpose and/or Means of processing.
2		4.2	**Establish the legal basis** as "Consent" or "Legitimate Use" for each process. *(Requires a Process Inventory covering also the data principals)*

4. Grounds for processing digital personal data

(1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,—

(a) for which the Data Principal has given her **consent;** or

(b) for certain **legitimate uses.**

(2) For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law

DPDPA Compliance List-2: DGPSI-Lite

3	5	5.1	Develop **appropriate Notice/s** indicating types of data collected, the purpose of collection with details of when the purpose terminates and how the data collected is related to the purpose. There may be one notice for each "Purpose" of collection. Legacy Data owners need to be given a separate Privacy Notice. Each Notice should be capable of being returned with verifiable consent. Notice and Consent are inter related.

5. Notice

(1) Every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal, informing her,—

(i) **the personal data** and **the purpose** for which the same is proposed to be processed;

(ii) the manner in which she may exercise her **rights** under sub-section (4) of section 6 and section 13; and

(iii) the manner in which the Data Principal may make a **complaint** to the Board, in such manner and as may be prescribed.

DPDPA Compliance List-3: DGPSI-Lite

4		5.2	Notice should indicate manner of exercising of Rights by Data Principals including power to withdraw consent, with a reminder of the duties of the data principal and consequences of withdrawal of consent
5		5.3	Notice should indicate manner of making complaint to DPB.
6		5.4	Notice should inform the availability of a manner of invoking the Grievance redress mechanism.
7		5.5	Notice should be available in 22 Scheduled Indian languages with an option for the data principal to chose.

5**. Notice**

((2) Where a Data Principal has given her consent for the processing of her personal data **before the date of commencement of this Act,**—

(a) the Data Fiduciary shall, as soon as it is reasonably practicable, give to the Data Principal a notice informing her,—

(i) the personal data and the purpose for which the same has been processed;

(ii) the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13; and

(iii) the manner in which the Data Principal may make a complaint to the Board, in such manner and as may be prescribed.

(b) the Data Fiduciary **may continue to process** the personal data until and unless the Data Principal withdraws her consent.

DPDPA Compliance List-4: DGPSI-Lite

8	6	6.1	Obtain consent which is Free, Specific, affirmative action, signifying agreement, (In the process organization needs to *generates the inventory of Processable Personal Data)*

6**. Consent**

(1) The consent given by the Data Principal shall be **free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement** to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.

(2) Any part of consent referred in sub-section (1) which constitutes an infringement of the provisions of this Act or the rules made thereunder or any other law for the time being in force shall be invalid to the extent of such infringement.

(3) Every request for consent under the provisions of this Act or the rules made thereunder shall be presented to the Data Principal in a clear and plain language, giving her the **option to access such request in English or any language** specified in the Eighth Schedule to the Constitution and providing the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for the purpose of exercise of her rights under the provisions of this Act..

DPDPA Compliance List-5: DGPSI-Lite

8	6	6.1	Obtain consent which is Free, Specific, affirmative action, signifying agreement, (In the process organization needs to g*enerates the inventory of Processable Personal Data)* *The consent must be unconditional and withdrawable*	6**. Consent** (4) Where consent given by the Data Principal is the basis of processing of personal data, such Data Principal shall have the **right to withdraw her consent** at any time, with the ease of doing so being comparable to the ease with which such consent was given. (5) The **consequences of the withdrawal** referred to in sub-section (4) shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal. (6) If a Data Principal withdraws her consent to the processing of personal data under sub-section (5), the Data Fiduciary shall, **within a reasonable time, cease and cause its Data Processors to cease** processing the personal data of such Data Principal unless such processing without her consent is required or authorised under the provisions of this Act or the rules made thereunder or any other law for the time being in force in India. Consent

DPDPA Compliance List-6: DGPSI-Lite

9		6.2	Establish procedure for using consents received from a Consent Manager	6. **Consent** (7) The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a **Consent Manager.** (8) The Consent Manager shall be a**ccountable to the Data Principal** and shall act on her behalf in such manner and subject to such obligations as may be prescribed. (9) Every Consent Manager **shall be registered** with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed

DPDPA Compliance List-7: DGPSI-Lite

10		6.3	Ensure documenting of the consent for prospective collection of personal data and tagging it with the relevant data set. *(Multiple notices and consent formats are required for multiple sources of collection)*
11		6.4	Ensure sending of notice to data principals of legacy holding of personal data, obtain consent and follow up for recording rejections, non-delivery, acceptances and no response. *(Requires discovery of personal data in the organization and its Data Processor's control)*

6. **Consent**

(10) Where a consent given by the Data Principal is the basis of processing of personal data and a question arises in this regard in a proceeding, the **Data Fiduciary shall be obliged to prove** that a notice was given by her to the Data Principal and consent was given by such Data Principal to the Data Fiduciary in accordance with the provisions of this Act and the rules made thereunder.

DPDPA Compliance List-8: DGPSI-Lite

12	7	7.1	Establish policy for legitimate use of personal data, with monitoring and control. *(Needs validation from the Top Management)*

7. Certain Legitimate Uses
-for the specified purpose for which the Data Principal has **voluntarily** provided her personal data…
… for fulfilling any **obligation under any law..**
… for **compliance with any judgment**
… for **responding to a medical emergency**
… or taking measures **to provide medical treatment or health services to any individual during an epidemic,**
for taking measures to ensure safety of, or provide assistance or services to, any individual during **any disaster, or any breakdown of public order.**
(i) for the **purposes of employment or those related to safeguarding the employer** from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee

DPDPA Compliance List-9: DGPSI-Lite

13	8	8.1	Ensure that the systems are in place to enable compliance with all aspects of the Act including the new the notifications that may be issued from time to time. *(The Data Fiduciary concept imposes a responsibility for compliance in letter and spirit)*

8. General Obligations of Data Fiduciary

(1) A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor.

(2) A Data Fiduciary may engage, appoint, use or otherwise involve a **Data Processor** to process personal data on its behalf for any activity related to offering of goods or services to Data Principals **only under a valid contract.**

(3) Where personal data processed by a Data Fiduciary is likely to be—

(a) used to make a **decision that affects the Data Principal;** or

(b) **disclosed** to another Data Fiduciary,
the Data Fiduciary processing such personal data shall **ensure its completeness, accuracy and consistency.**

DPDPA Compliance List-10: DGPSI-Lite

14		8.2	Ensure availability of appropriate contract for all downstream data processors and s with upstream vendors. *(Requires systematic review of every business contract)*
15		8.3	Establish appropriate technical and organizational measures for effective observance of compliance. *(This is an open ended and dynamic requirement and related to a risk assessment)*

8. General Obligations of Data Fiduciary

(4) A Data Fiduciary shall implement **appropriate technical and organisational measures to ensure effective observance of the provisions of this Act** and the rules made thereunder.

(5) A Data Fiduciary shall **protect personal data** in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent **personal data breach.**

(6) In the event of a **personal data breach**, the Data Fiduciary shall give the Board and each affected Data Principal, **intimation** of such breach in such form and manner as may be prescribed.

(7) A Data Fiduciary shall, **unless retention is necessary** for compliance with any law for the time being in force,—

(a) **erase personal data,** upon the Data Principal **withdrawing her consent** or as soon as it is reasonable to assume that the **specified purpose is no longer being served,** whichever is earlier; and

(b) cause its **Data Processor to erase** any personal data that was made available by the Data Fiduciary for processing to such Data Processor

DPDPA Compliance List-11: DGPSI-Lite

16		8.4	Ensure protection of personal data with self and with data processor with reasonable security safeguards. *(This is an open ended and dynamic requirement and related to the preservation of confidentiality, integrity and availability of subject personal data.)*
17		8.5	Establish appropriate policy to identify, investigate, respond and report a personal data breach to the DPB/Data Principal. *(Requires an appropriate Incident Identification, Reporting, evaluation and response system)*

8. General Obligations of Data Fiduciary

(8) The purpose referred to in clause (a) of sub-section (7) shall be deemed to no longer be served, if the Data Principal does not—

(a) approach the Data Fiduciary for the performance of the specified purpose; and

(b) exercise any of her rights in relation to such processing, for such time period as may be prescribed, and different time periods may be prescribed for different classes of Data Fiduciaries and for different purposes.

DPDPA Compliance List-12: DGPSI-Lite

18		8.6	Ensure data retention is linked to purpose of collection. *(Requires erasure or archival of data when the purpose is terminated or consent withdrawn)*
19		8.7	Publish the business contact information of the DPO/Compliance officer.
20		8.8	Establish an appropriate Grievance Redressal mechanism. *(Requires a responsive complaint handling system with negotiation, intervention of ombudsman and mediation)*

8. General Obligations of Data Fiduciary

(9) A Data Fiduciary shall publish, in such manner as may be prescribed, the **business contact information of a Data Protection Officer**, if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the questions, if any, raised by the Data Principal about the processing of her personal data.

(10) A Data Fiduciary shall establish an effective mechanism to **redress the grievances** of Data Principals.

(11) For the purposes of this section, it is hereby clarified that a Data Principal shall be considered as not having approached the Data Fiduciary for the performance of the specified purpose, in any period during which she has not initiated contact with the Data Fiduciary for such performance, in person or by way of communication in electronic or physical form.

DPDPA Compliance List-13: DGPSI-Lite

21	9	9.1	In case of minors or persons with disability to provide own consent, obtain verifiable consent from the parent or guardian. *(Requires age-gating and identification of data principals to whom the tag of minor or disabled can be applied)*

9. Processing Personal Data of Children

(1) The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed.

(2) A Data Fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child.

(3) A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

DPDPA Compliance List-14: DGPSI-Lite

22		9.2	Establish policies to restrict the behaviour monitoring or targeted advertising of the minor. *(Requires management of activities of Advertisers)*	9. Processing Personal Data of Children (4) The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child by such classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed. (5) The Central Government may, if satisfied that a Data Fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe, notify for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations under sub-sections (1) and (3) in respect of processing by that Data Fiduciary as the notification may specify.

DPDPA Compliance List-15: DGPSI-Lite

23	10	10.1	Identify if the organization is a Significant Data Fiduciary (SDF) and document the reasons thereof. *(Err on the safe side)*

10. Additional obligations of Significant Data Fiduciary

(1) The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of such relevant factors as it may determine, including

(a) the volume and sensitivity of personal data processed;
(b) risk to the rights of Data Principal;
(c) potential impact on the sovereignty and integrity of India;
(d) risk to electoral democracy;
(e) security of the State; and
(f) public order

DPDPA Compliance List-16: DGPSI-Lite

24		10.2	If organization is a SDF appoint **a Data Protection Officer** with relevant credentials. *(Requires understanding of what is required to be a good DPO in India. A qualification in GDPR compliance is not necessarily a qualification in DPDPA. It may be a good practice to retain access to external DPO consultants to meet exigencies to assist the DPO)*

10. Additional obligations of Significant Data Fiduciary

(2) The Significant Data Fiduciary shall—
(a) appoint a Data Protection Officer who shall—
(i) represent the Significant Data Fiduciary under the provisions of this Act;
(ii) be based in India;
(iii) be an individual responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary; and
(iv) be the point of contact for the grievance redressal mechanism under the provisions of this Act;

DPDPA Compliance List-17: DGPSI-Lite

25		10.3	If organization is a SDF, appoint an **independent Data auditor** with relevant credentials.	**10. Additional obligations of Significant Data Fiduciary** (b) appoint an independent data auditor to carry out data audit, who shall evaluate the compliance of the Significant Data Fiduciary in accordance with the provisions of this Act; and (c) undertake the following other measures, namely:— (i) periodic Data Protection Impact Assessment, which shall be a process comprising a description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals, and such other matters regarding such process as may be prescribed; (ii) periodic audit; and (iii) such other measures, consistent with the provisions of this Act, as may be prescribed.
26		10.4	If organization is a, SDF, establish a policy for conducting **periodic Data Protection Impact Assessment** an Periodic audit for relevant processes.	

DPDPA Compliance List-18: DGPSI-Lite

27	11	11.1	Establish measures to provide **right to access** to a data principal and to respond promptly with appropriate response. *(Note that if any adverse information has been hidden in the notice, it may get revealed in the summary of processing to be revealed*

11.Right to access information about personal data.

.. (a) a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data;

(b) the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared; and

(c) any other information related to the personal data of such Data Principal and its processing, as may be prescribed.

DPDPA Compliance List-19: DGPSI-Lite

28	12	12.1	Establish measures to provide **right to correction and erasure**, to a data principal and to respond promptly with appropriate response. *(Note that the data principal has a duty to provide correct information and correct wrong information if already held)*

12. Right to correction and erasure of personal data

.. (1) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force

… the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.

DPDPA Compliance List-20: DGPSI-Lite

29	13	13.1	Inform and educate the Data Principal on the existence and use of **grievance redressal mechanism** and its access through the consent manager.

13. Right of grievance redressal

(1) A Data Principal shall have the right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager in respect of any act or omission of such Data Fiduciary or Consent Manager regarding the performance of its obligations in relation to the personal data of such Data Principal or the exercise of her rights under the provisions of this Act and the rules made thereunder.

(2) The Data Fiduciary or Consent Manager shall respond to any grievances referred to in sub-section (1) within such period as may be prescribed from the date of its receipt for all or any class of Data Fiduciaries.

(3) The Data Principal shall exhaust the opportunity of redressing her grievance under this section before approaching the Board

DPDPA Compliance List-21: DGPSI-Lite

30	14	14.1	Establish appropriate measures to provide **right to nomination** and necessary measures to act there on at the appropriate time. *(This requires an elaborate system of claims management)*

14. Right to nominate.

(1) A Data Principal shall have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal in accordance with the provisions of this Act and the rules made thereunder.

(2) For the purposes of this section, the expression "incapacity" means inability to exercise the rights of the Data Principal under the provisions of this Act or the rules made thereunder due to unsoundness of mind or infirmity of body

DPDPA Compliance List-22: DGPSI-Lite

31	15	15.1	Ensure that the data principals are appropriately informed about their duties under the Act. *(It would be a good practice to obtain an undertaking)*	**15. Duties of Data Principal.** A Data Principal shall perform the following duties, namely:— (a) comply with the provisions of all applicable laws for the time being in force while exercising rights under the provisions of this Act; (b) to ensure not to impersonate another person while providing her personal data for a specified purpose; (c) to ensure not to suppress any material information while providing her personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities; (d) to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board; and (e) to furnish only such information as is verifiably authentic, while exercising the right to correction or erasure under the provisions of this Act or the rules made thereunder.

DPDPA Compliance List-23: DGPSI-Lite

32	16	16.1	Ensure to keep track of any directions from Data Protection Board or relevant sectoral regulators about restrictions for personal data transfer outside India.

16. Processing of personal data outside India

(1) The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.

(2) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof.

DPDPA Compliance List-24: DGPSI-Lite

33	17	17.1	Establish appropriate measures to identify and avail exemptions available with strict observance of attached conditions and limitations. *(Note that all exemptions have their own individual limitations, and a strict adherence is required)*	17. Exemptions 17(1),17(2),17(3),(17(4),17(5) … (d) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India; .. merger or amalgamation .. defaulted in payment due on account of a loan or advance taken from a financial institution

DPDPA Compliance List-25: DGPSI-Lite

34	28	28.1	Establish measures to promptly receive and respond to any communication received from the Data Protection Board, participate in the inquiry process and avail of the voluntary undertaking benefit where available.

28: Procedure to be followed by Board.

The Board may, on receipt of an intimation or complaint or reference or directions as referred to in sub-section (1) of section 27, take action in accordance with the provisions of this Act and the rules made thereunder…..

The Board may accept a voluntary undertaking in respect of any matter related to observance of the provisions of this Act from any person at any stage of a proceeding under section 28.

DPDPA Compliance List-26: DGPSI-Lite

35	30	30.1	Establish measures to receive directives from Data Protection Board and respond appropriately and without delay to comply with the order or otherwise respond to it with appeal, or representation for review or for proposing voluntary undertaking

30: Orders passed by Appellate Tribunal to ne executable as decree

1) An order passed by the Appellate Tribunal under this Act shall be executable by it as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

DPDPA Compliance List-27: DGPSI-Lite

36	32	32.1	Establish measures to structure and propose voluntary undertaking where required	**32: Voluntary Undertaking** (1) The Board may accept a voluntary undertaking in respect of any matter related to observance of the provisions of this Act from any person at any stage of a proceeding under section 28. (2) The voluntary undertaking referred to in sub-section (1) may include an undertaking to take such action within such time as may be determined by the Board, or refrain from taking such action, and or publicising such undertaking. (3) The Board may, after accepting the voluntary undertaking and with the consent of the person who gave the voluntary undertaking vary the terms included in the voluntary undertaking. (4) The acceptance of the voluntary undertaking by the Board shall constitute a bar on proceedings under the provisions of this Act as regards the contents of the voluntary undertaking, except in cases covered by sub-section (5). (5) Where a person fails to adhere to any term of the voluntary undertaking accepted by the Board, such breach shall be deemed to be breach of the provisions of this Act and the Board may, after giving such person an opportunity of being heard, proceed in accordance with the provisions of section 33

Compliance is a Journey

- Earlier one starts, better it is…
- Process Inventory and Personal Data Inventory is a pre-requisite
- Process centric consent is required with control on data minimization and data retention minimisation.
- Follow the DGPSI framework for better focus
- Consider as if the Act is effective today as Due Diligence under ITA 2000.

Thank You…Questions?

- naavi@fdppi.in
- www.fdppi.in
- www.Naavi.org