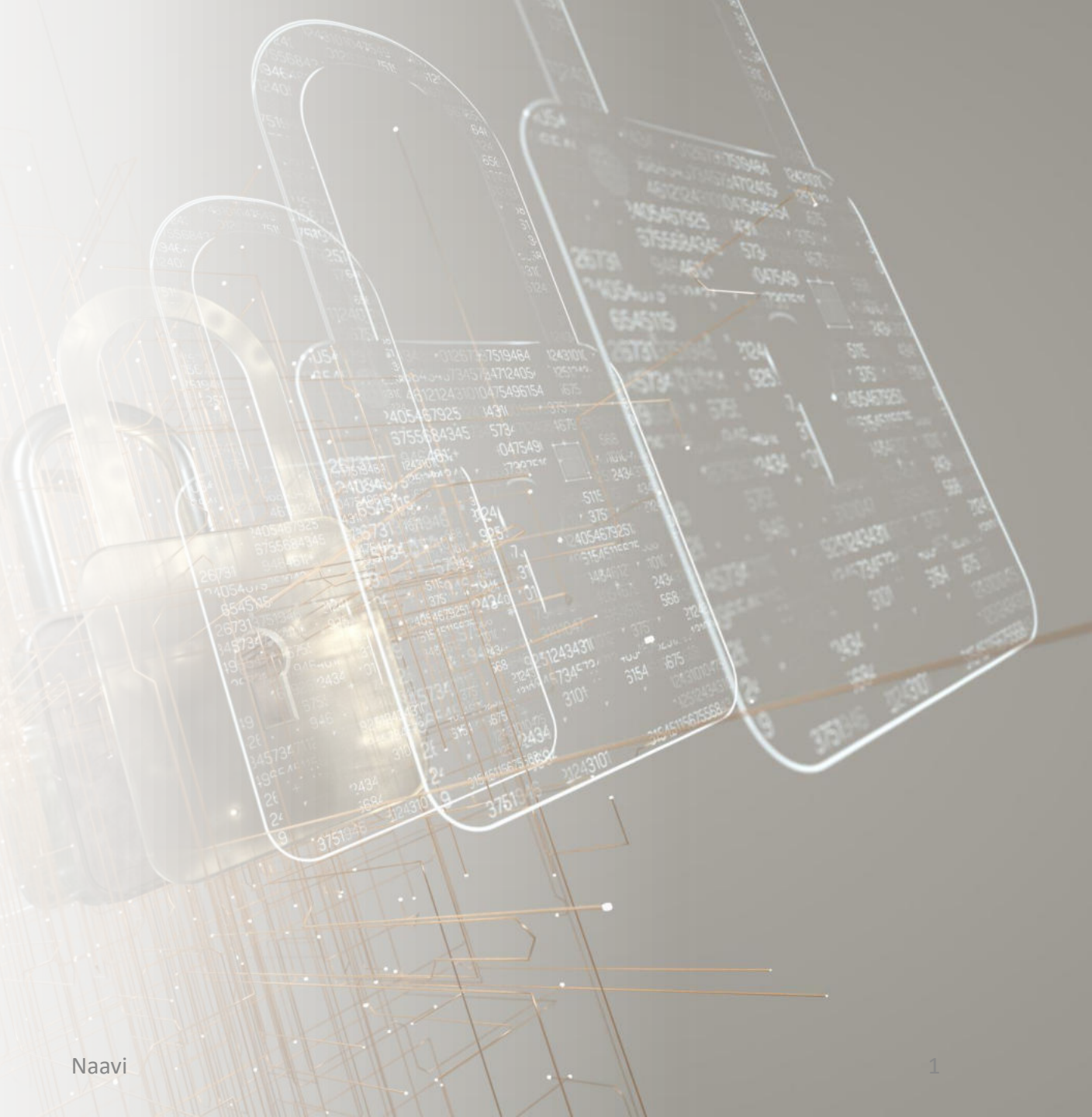
Introduction to the Concept of Data Protection and Structure and Key Definitions vis-à-vis DPDPB2022

21st November 2022



Agenda

- Concept of Data Protection
- Quick recall of the Concept of Privacy
- How Privacy becomes Data Protection
- Key Aspects of Data Protection Act

Two Dimensions of Data Protection

- Data Protection has two main dimensions
  - Protection of Non Personal Data
    - Reflected in Information Security or Cyber Security
  - Protection of Personal Data
    - Reflected in Privacy Protection and some times also referred to as Data Privacy or Information Privacy
- Data Privacy or Information Privacy is a Human Rights Concept as an extension of Right to Privacy
    - Information Security is a Quality and Security concept for IT professionals

Data is changing its profile with Technology

- Data is no longer limited to Oral and Written. It has gone digital
  - Digital Data is the most prominent form in which “Data” or “Information” is found in this world
- According to Theory of Data
  - Data is created by Technology but interpreted by Humans
- Technology view of Data is as 0s and 1s…either organized or disorganized
- Human View of Data is as Text, Audio, Video or Smell, Touch and Taste
  - Provided the right kind of interpreting and interacting peripherals are available

Technology and Human Perspective of Protection

- **Protecting Data from Technical Perspective**
  - Ensure only authorized persons have access (Confidentiality)
  - Ensure only authorized persons can modify (Integrity)
  - Ensure that authorized persons will not be denied access (Availability)
    - Emphasis of Information security is protection of Data (Both personal ad Non Personal) the wrongful access or modification etc of which can cause harm of certain types such as financial loss, reputation loss, loss of life, loss of employment etc to any entity

Technology and Human Perspective of Protection

- **Protecting Data from Human Perspective**
  - Ensure only authorized persons have access (Confidentiality)
  - Ensure only authorized persons can modify (Integrity)
  - Ensure that authorized persons will not be denied access (Availability)
  - Ensure that Unauthorized access does not lead to a harm to the Privacy of a human
    - Emphasis of Privacy Protection is protection of “Personal Data”, the wrongful disclosure of which can cause harm of certain types such as impairment of ability to act freely besides the other harms to an individual

New Technology poses new challenges..

- *Quantum Computing*
  - *The power of attack can increase and Strategies for defense has to keep pace*
  - *Super positioning and Entanglement create new opportunities*
- *Big Data*
  - *Requires raw data of large size without adversely affecting information security or Privacy*
  - *Data Analytics and Discovery of new uses of data is an essential part of Big Data Business*
- *Artificial Intelligence*
  - *Needs to work within limits to prevent rogue software causing damages to humanity*
  - *Unsupervised Machine learning could lead to bias*
- *IoT*
  - *Ubiquitous presence of Alexa, Wearable watches, Smart TVs, enable collection of data from private moments with both positive and negative connotations which require security measures.*

New Technology poses new challenges

- *Medical Implants*
  - *Intrusive and some times available for external connectivity could cause life threatening situations*
  - *Brain computer interfaces raise the level of security risk to unprecedented levels*
- *Meta Verse*
  - *Takes Social media to higher levels of immersive experience with heightened possibilities of Cyber hypnotism and related consequences*
- *Blockchain*
  - *A technology platform that distributes data to many more than who have the need to know though controlled by encryption.*
- *Remote activity*
  - *For Data Storage, Processing and Operation*

Concept of Privacy

Sarve Sve Sve Grihe Raja (Every Man is a king in his own house) -14th century text

- Narayana Pandita, Panchatantra/Hitopadesha

Home is the Castle… No unauthorized intrusion into a person's home

- Kharaksingh vs State of UP (AIR 1963)

Right to privacy is implicit on the Right to life and liberty (article 21)

- R Rajagopalan Vs State of Tamil Nadu

Right to Privacy is a fundamental Right under Article 21

- 9 member bench of Supreme Court-24th August 2017 (Puttaswamy judgement)
- "Right to be left alone"

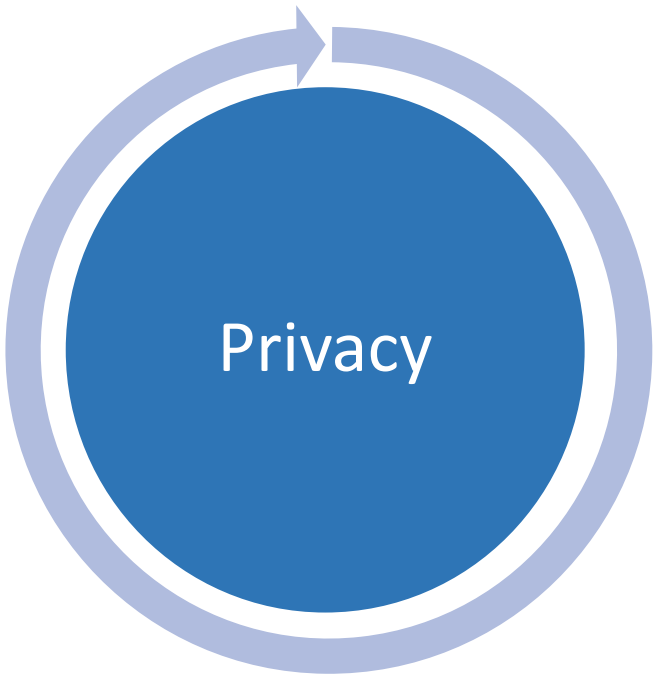
State of mind of an individual

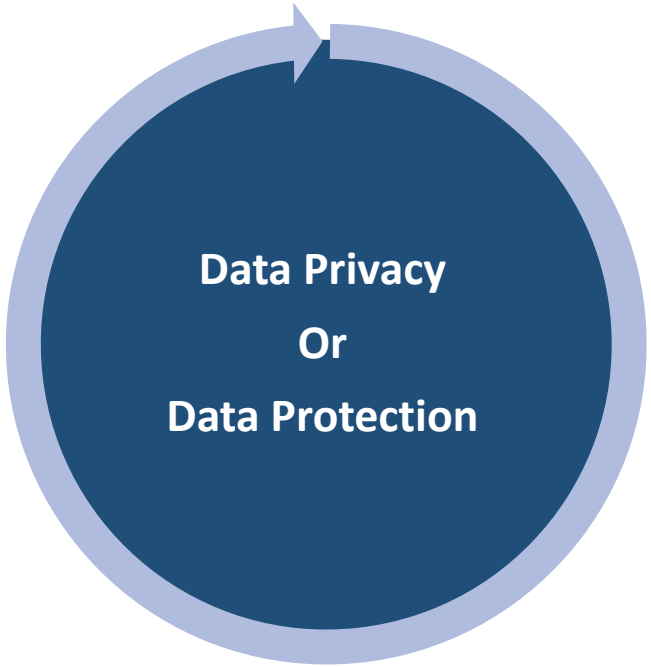
- Can change from individual to individual
- Can change from time to time for the same individual
- Defining the Right and framing a law to protect it is impossible

Privacy as A Right of Choice

- The impossibility of protecting the “State of Mind” of an individual by law has resulted in the protection of right of privacy being re-defined …and limited to Digital privacy

Privacy of an individual and Data Privacy





Protecting the Privacy of an individual by following certain measures related to the processing of personal data

A Human Rights concept… State of mind of an individual…feeling of being let alone

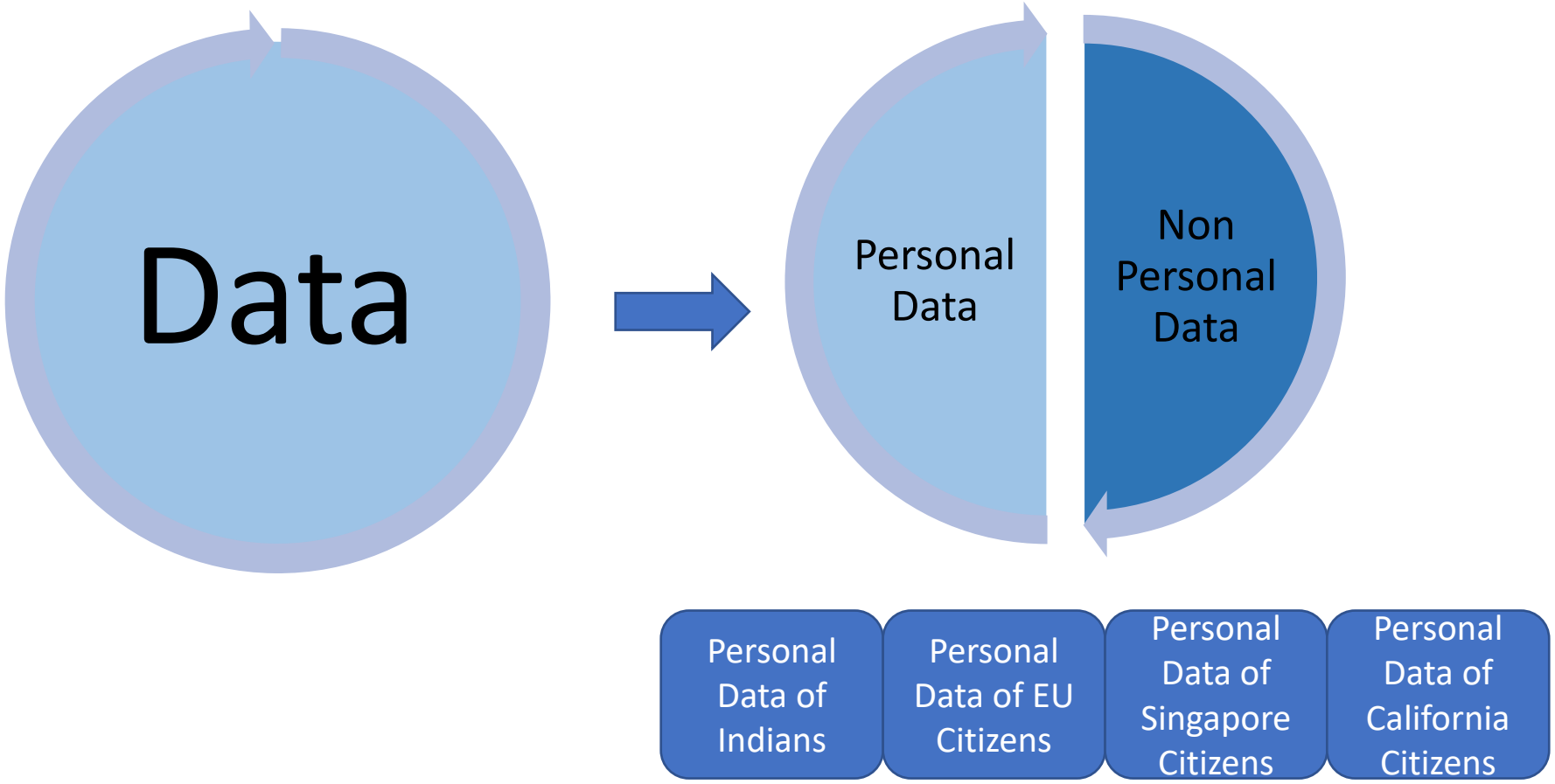
An IT concept involving “technical controls” and “written policies” and an “enforcement/ Governance” system

The Current operating definition

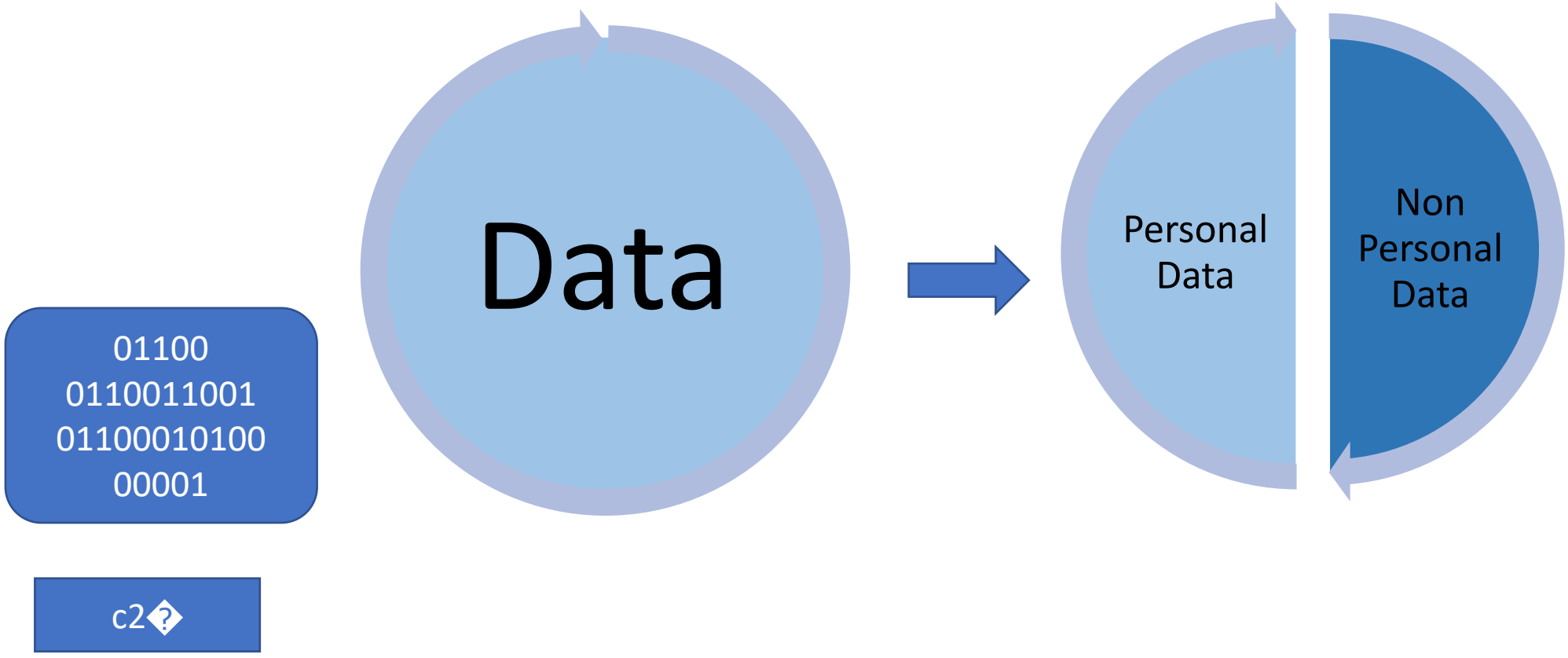
- Right to Privacy Means
  - *“Right of self determination and enforcement*
  - *of a natural person*
  - *on how the personal data may be shared and*
  - *used by a recipient.”*

Naavi

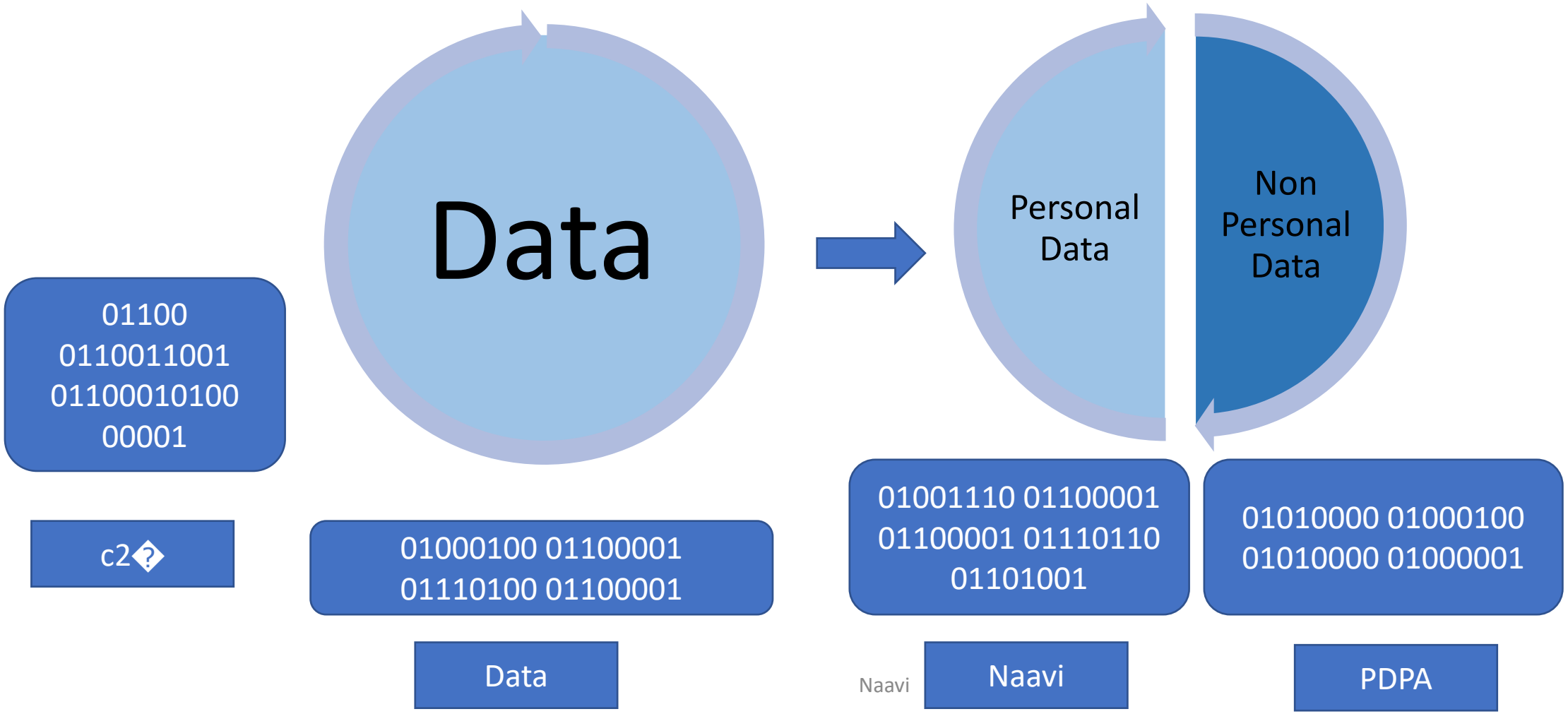
Data Categories from Protection perspective



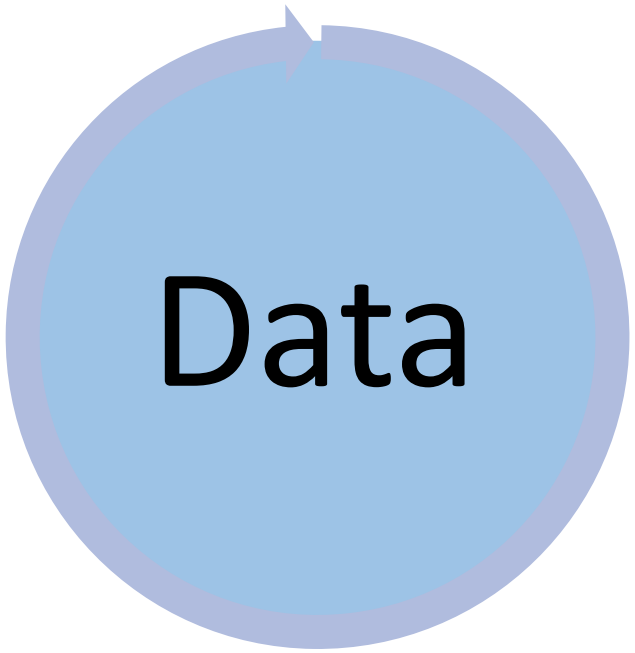
Avatars of Data…

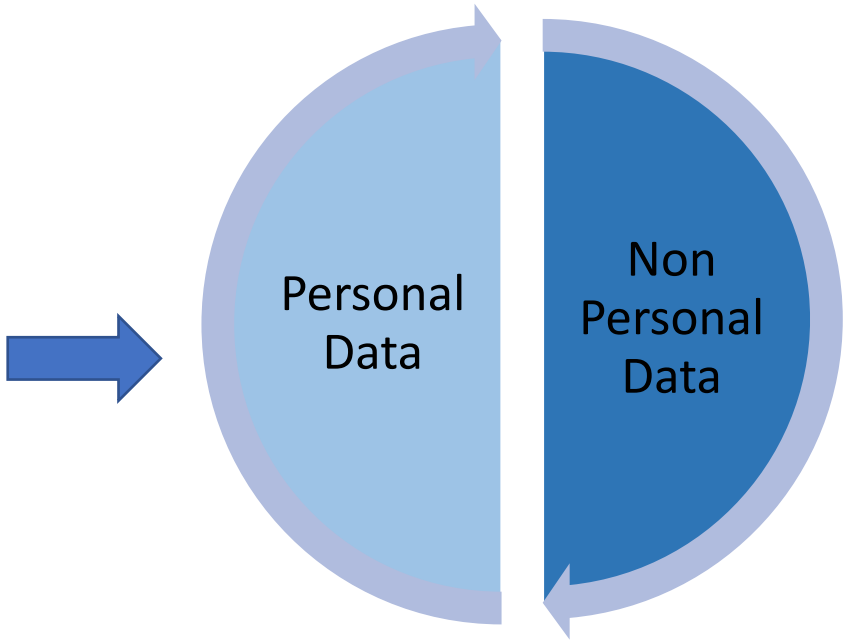


When binary data is organized, they acquire a capability to be interpreted by device into Text or otherwise



Which Data is Personal or Non Personal or which data interpreting device to be used is the Choice of the human





"Data is in the beholder's eyes" ..Theory of Data

01100 0110011001 0110001010000001

c2

01000100 01100001 01110100 01100001

Data

1147237473

01001110 01100001 01100001 01110110 01101001

Naavi

336641226345

01010000 01000100 01010000 01000001

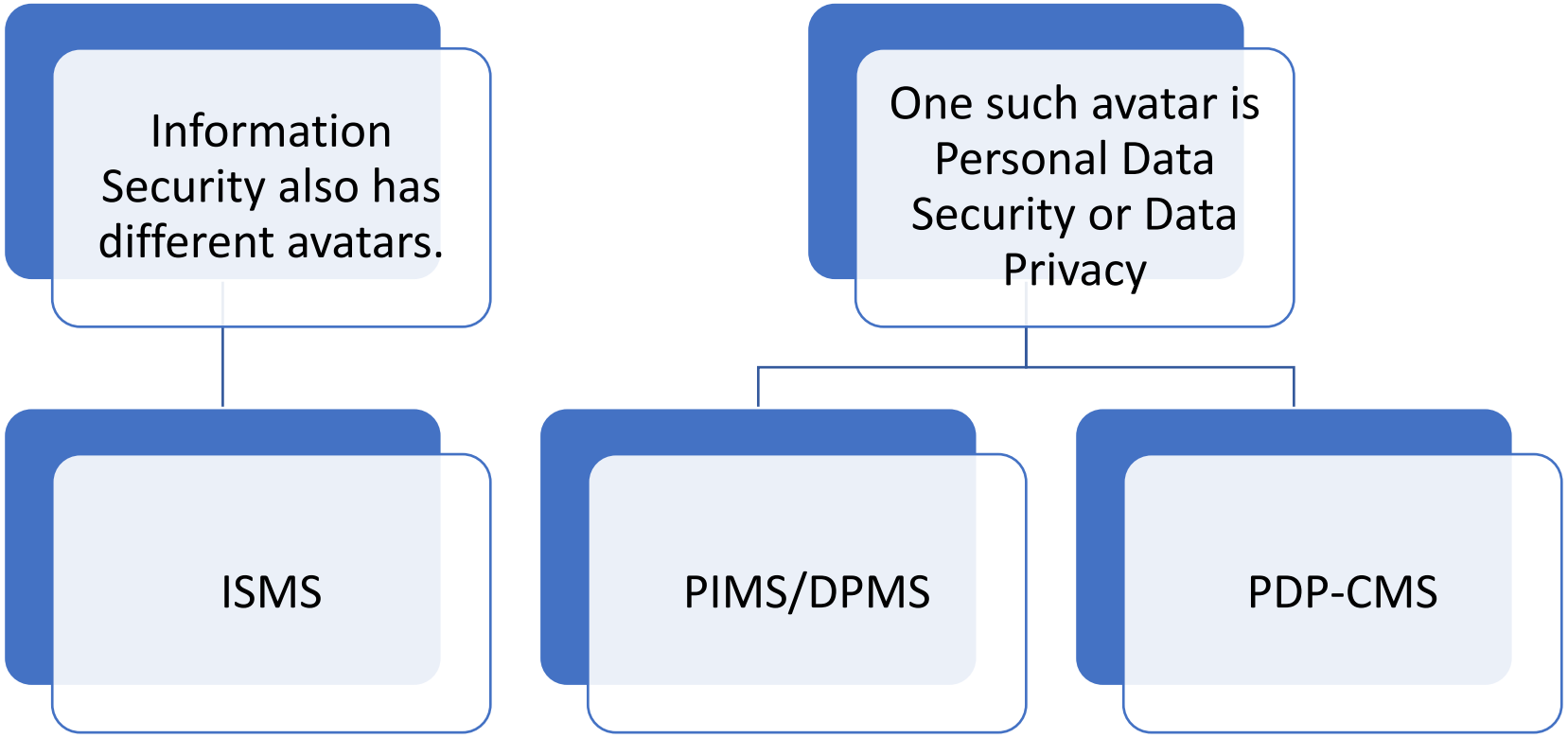
PDPA

1346654273

Theory of Data

- **Data is in the beholder's eyes**
  - Data is created by technology as a sequence of binary values expressed on a platform that may hold the binary values
- **Data is Dynamic and exists in different forms**
  - Data Life cycle is reversible
  - Chaotic arrangement of binaries to organized sequence of binaries which a human can interpret as some kind of experience.
  - Like a Kaleidoscope, binary arrangements can be re-arranged to create new forms of data
- **Data accumulates value as it transforms from one form to another**
  - The value of data belongs to the person who created the given state of the Data.

Evolution of Information Security Management…



Structure of DPDPB 2022 (Draft released on 16th November 2022)

30 sections spread over 6 chapters

Chapter	Title	Sections
1	Preliminary	1-4
2	Obligations of Data Fiduciary	5-11
3	Rights and Duties of Data Principal	12-16
4	Special Provisions	17-18
5	Compliance Framework	19-25
6	Miscellaneous	26-30
Schedule1	Penalties	

Essence of the New Bill

- Scope limited to Digital Personal Data Protection and Not “Privacy Protection”
- Bill is kept simple and details will come in the subordinate legislation
  - Section 3(1) says
    - “provisions of this Act” shall be read as **including a reference to Rules** made under this Act.

Applicability

- Processing of Digital personal data within the territory of India where Personal data is
  - collected on line
  - Collected off-line and digitized
- Processing of Digital personal data outside the territory of India if it is
  - In connection with any profiling or activity of offering goods or services to Data Principals within the territory of India
- Not applicable to
  - Non automated processing, Offline personal data, processed by an individual for personal or domestic purpose and if it has been in existence for over 100 years.
    - "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**

Exemption for BPOs and Start Ups

- 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.
- The Central Government may by notification, having regard to the volume and nature of personal data processed, **notify** certain Data Fiduciaries or class of Data Fiduciaries as Data Fiduciary to whom the provisions of Section 6, (notice) sub-sections (2) and (6) of section 9, sections 10, 11(obligations) and 12(Right to information) of this Act shall not apply.

Notice

- To be obtained on or before collection
  - Consent before commencement of the Act…the Data Fiduciary must give to the Data Principal an itemised notice in clear and plain language containing a description of personal data of the Data Principal collected by the Data Fiduciary and the purpose for which such personal data has been processed, as soon as it is reasonably practicable.
  - Should be accessible in other schedule languages

Consent

- Free consent by affirmative action
  - Any part of consent referred in sub-section (1) which constitutes an infringement of provisions of this Act shall be invalid to the extent of such infringement.
- Consent is Withdrawable
- Deemed consent
  - Employment, Public interest, law enforcement
  - Health Emergency
  - Judicial requirement
  - Disaster or breakdown of public order
  - Public interest including prevention or detection of fraud, Information security, debt recovery, mergers and acquisitions
  - Processing of Publicly available personal data

Definition of Harm

- “Harm”, in relation to a Data Principal, means -
  - a. any bodily harm; or
  - b. distortion or theft of identity; or
  - c. harassment; or
  - d. prevention of lawful gain or causation of significant loss;
    - Loss ang Gain defined in monetary terms

Free Consent in the era of neuro Technology

- Developments of Neuro Technology where Brain Computer Interfaces are developed
  - As part of Medical Science
  - As part of Gaming
- Ability of the interfaces to intrude into neuro space without surgical implants and through sound waves pose a distinct risk that
  - Free Consent of an individual may not free consent at all and could be a neuro manipulated content
    - We need to move from protection of Privacy Rights to Protection of Neuro Rights

Roles

- Data Fiduciary
  - “Data Fiduciary” means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;
- Data Processor
  - “Data Processor” means any person who processes personal data on behalf of a Data Fiduciary;
- Data Protection officer
  - “Data Protection Officer” means an individual appointed as such by a Significant Data Fiduciary under the provisions of this Act;
- Data Auditor
  - One appointed to evaluate the compliance of the Significant Data Fiduciary with provisions of this Act;

Significant Data Fiduciary

- Recognition on several parameters
  - Volume and sensitivity of personal data processed
  - Risk of harm to the Data Principal
  - **Potential impact on the sovereignty and integrity of the nation**
  - **Risk to electoral democracy**
  - **Security of State**
  - **Public order**
- Appoint a DPO
- Appoint an Independent Data Auditor

Consent manager

- Consent Manager" is a Data Fiduciary which enables a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform
- is accountable to the Data Principal and acts on behalf of the Data Principal.
  - 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.

Obligations of a Data Fiduciary

- Processing is lawful if it is not expressly forbidden by law but it has to be processed only as per this Act and with consent deemed or otherwise.
- Shall comply with the provisions of the Act
  - Maintain data accuracy particularly when the data is used to make a decision about the individual
  - Appropriate technical and organizational measures to ensure effective adherence with the provisions of the Act (Compliance by design?)
  - Reasonable Security to prevent data breach
  - Publish the business contact information of the DPO
  - Obtain parental consent in the case of Minors, shall not cause harm to a child

Rights of a Data Principal

- Right to Information about personal data
- Right to correction and erasure of personal data
- Right to Grievance Redressal
- Right to Nominate

Duties of Data Principal

- (1) A Data Principal shall comply with the provisions of all applicable laws while exercising rights under the provisions of this Act.
- (2) A Data Principal shall not register a false or frivolous grievance or complaint with a Data Fiduciary or the Board.
- (3) A Data Principal shall, under no circumstances including while applying for any document, service, unique identifier, proof of identity or proof of address, furnish any false particulars or suppress any material information or impersonate another person.
- (4) A Data Principal shall furnish only such information as is verifiably authentic while exercising the right to correction or erasure under the provisions of this Act

Special Provisions

- Transfer of Personal Data outside India
  - The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified.

Exemptions

- (1) The provisions of Chapter 2 except sub-section (4) of section 9, Chapter 3 and Section 17 of this Act shall not apply where:
  - (a) the processing of personal data is necessary for enforcing any legal right or claim;
  - (b) the processing of personal data by any court or tribunal or any other body in India is necessary for the performance of any judicial or quasi-judicial function;
  - (c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law;
  - (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.

Exemptions

- (2) The Central Government may, by notification, exempt from the application of provisions of this Act, the processing of personal data:
  - a. by any instrumentality of the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these; and
  - (b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with standards specified by the Board.
- (3) The Central Government may by notification, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries as Data Fiduciary to whom the provisions of Section 6, sub-sections (2) and (6) of section 9, sections 10, 11 and 12 of this Act shall not apply.
- (4) The provisions of sub-section (6) of section 9 of this Act shall not apply in respect of processing by the State or any instrumentality of the State.

Regulatory Agency

- **Data Protection Board** to be established
  - To determine non compliance
  - To conduct inquiry based on complaints received
  - May make use of police for investigation
  - To Issue Corrective directions
- May review its own order and conduct hearing by a larger group
- Appeal against the Board lies with High Court
- No Civil Court shall have jurisdiction
- ADR may be suggested
- May accept “Voluntary Undertaking” to comply
- May levy penalty

Penalties

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

Summary

- Truncated Bill
- Dependent on subordinate legislation
- Controversial provisions avoided
- Addresses only Digital personal data protection and not “Privacy”
- Rights curtailed with no Right to Portability and Right to Forget
- Sand Box system not presently available
- Algorithmic transparency not presently mandated
- DTS not presently mandated
- Details of DPO requirements or Data Audit requirements not indicated
- Codes of Practice provision not indicated

Thank You

naavi@naavi.org

www.naavi.org

+919343554943