Digital Data Protection Bill 2022
Explained

Dr. Sunil T T

College of Engineering Attingal

suniltt@gmail.com

December 14, 2022

Background: Global Scenario

Growth of Internet

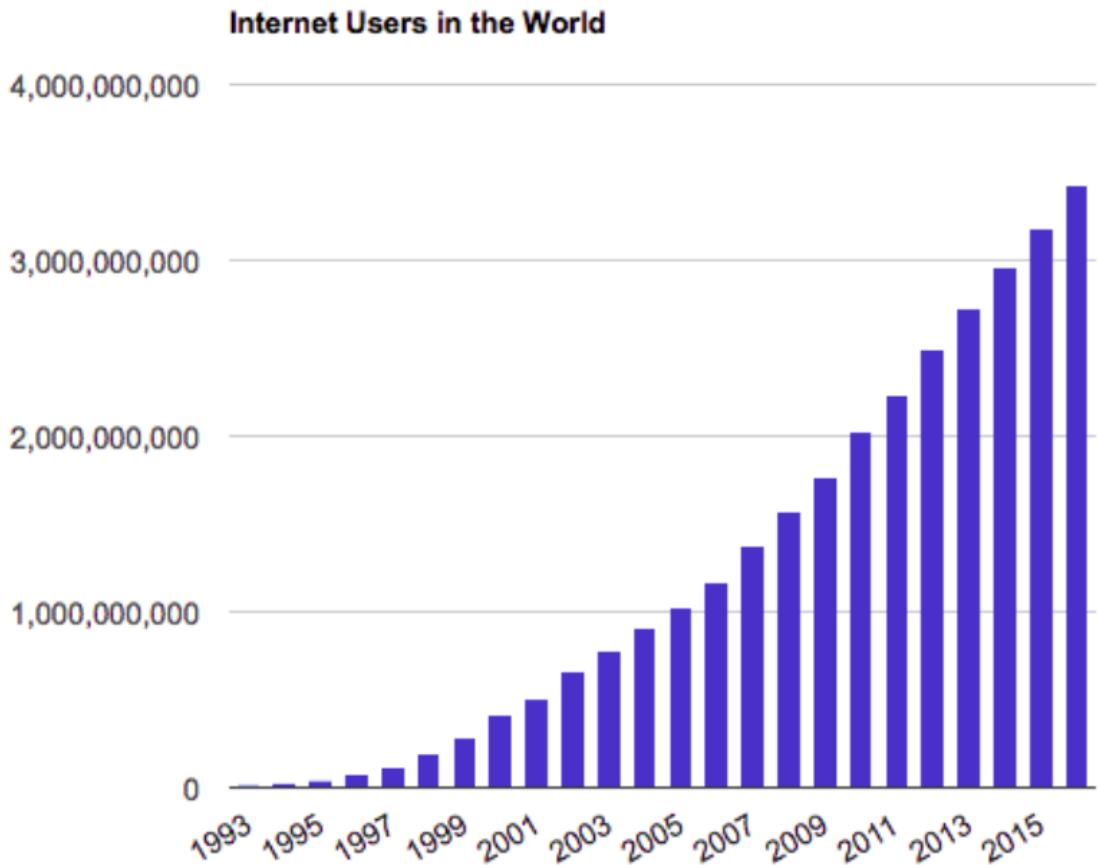
Major Data Breaches

Need for data protection

GDPR, US and Chinese laws

Background:Growth of Internet

In india the current internet user base is 76 crore and is expected to reach 120 crore.



Data reported by http://www.internetlivestats.com/internet-users/

Background:Major Data Breaches in Recent Times

Yahoo data breach (2013)

First American Financial Corporation data breach (2019)

Equifax data breach (2017)

Marriott International data breach (2018)

Adult FriendFinder Networks data breach (2016)

U.S. Office of Personnel Management data breach (2015)

Facebook data breach (2019)

Cambridge Analytica incident

European, US and Chinese Laws

European Union Model:

- GDPR : focuses on a comprehensive data protection law for processing of personal data.
- In the EU, the right to privacy is enshrined as a fundamental right
- GDPR seeks to protect an individual's dignity and her right over the data she generates.

US Model:

- Not linked to privacy
- Limited sector-specific regulation
- The activities and powers of the government vis-a-vis personal information are well-defined and addressed by broad legislation such as the Privacy Act, the Electronic Communications Privacy Act, etc

China Model:

- Personal Information Protection Law (PIPL) 2021
- Protection against misuse of personal data
- Data categorized on on levels of importance-restricts cross border transfer

Background:Indian Scenario

Justice K. S. Puttaswamy (Retd) vs Union of India 2017:

In August 2017, a nine-judge bench of the Supreme Court held that Indians have a constitutionally protected fundamental right to privacy that is an intrinsic part of life and liberty under Article 21.

B.N. Srikrishna Committee 2017:

The Report has a wide range of recommendations to strengthen privacy law in India including restrictions on processing and collection of data, Data Protection Authority, right to be forgotten, data localization etc

Data protection bill 2019

The Personal Data Protection Bill, 2019 was introduced in Lok Sabha on December 11, 2019.

It was sent to a joint parliamentary committee

Govt. withdrew the bill later

Some of the reasons , opposition from major stakeholders, compliance difficulties ,Issues with Data Localization : Alleged blanket exemption to Govt agencies

Data protection Bill 2022

Watered down version of 2019 bill available for public comments

Definitions

- Data
- Data Principal
- Data Fiduciary
  - Significant Data Fiduciary
- Data Processor
- Data Protection Officer
- Gain
- Harm
- Loss
- Personal data
- Personal data breach

Definitions

Data Fiduciary

who decides the purpose of data processing

Data Processor

who processes data on behalf

Data Principal

Individual whose data is processed

Data Processing

Personal data and Sensitive Personal Data

What is Data ?

DPDP act defines data as

A representation of

- information
- facts
- opinions
- instructions

in a manner suitable for communication, interpretation or processing by humans or by automated means

Personal Data is defined as

any data about an individual who is identifiable by or in relation to such data.

Comment: This is some what vague, compared to European GDPR, The Bill does not distinguish between personal data, and sensitive personal data, which is a crucial distinction recognition that some types of data require stricter and stronger protection than others

Personal Data Breach

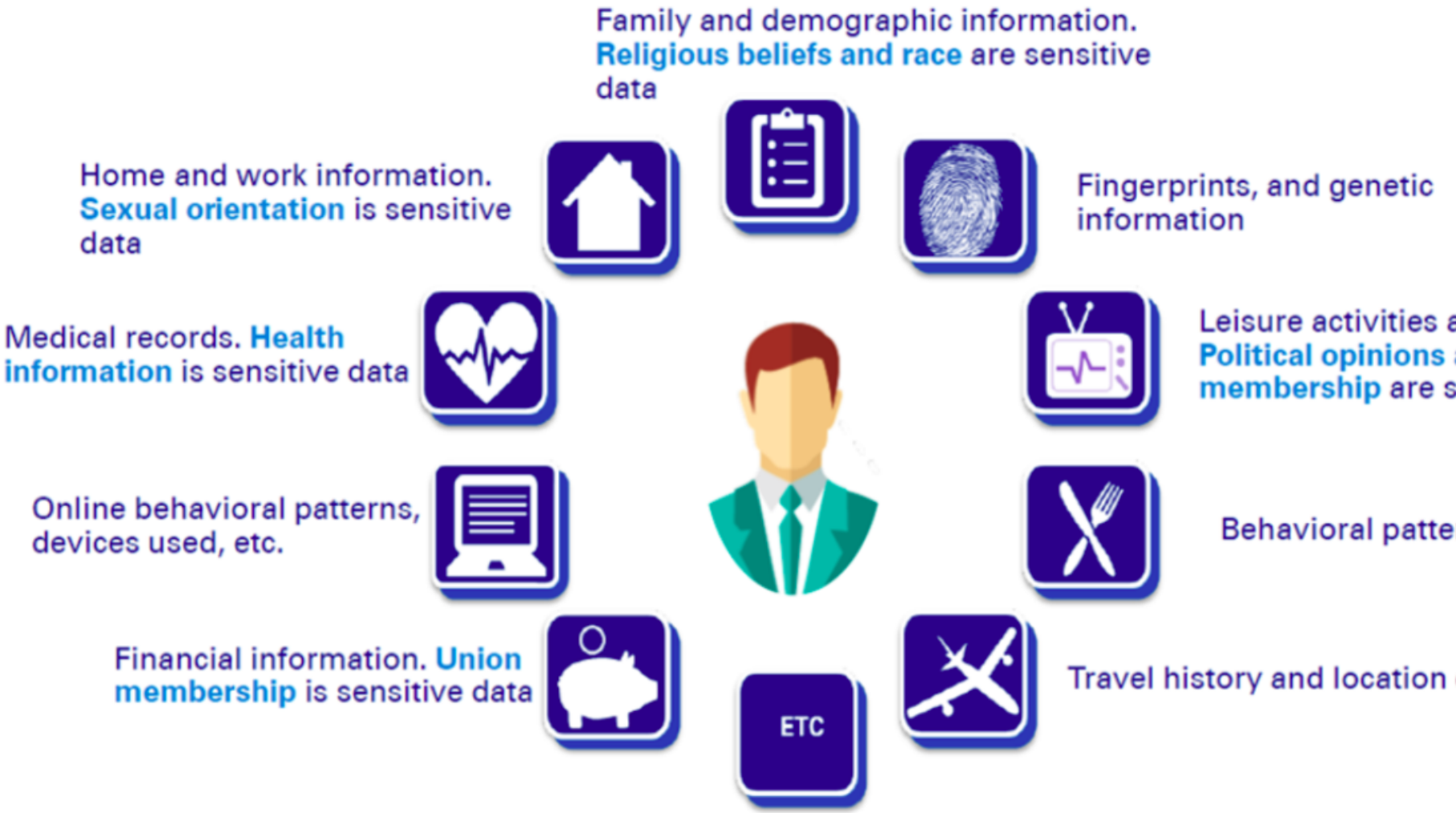
Any unauthorised

processing of personal data or	use,
accidental disclosure,	alteration,
acquisition,	destruction of or loss of access to personal data,
sharing,	

that compromises the confidentiality, integrity or availability of personal data.

Comment: Bill does not mention unreasonable surveillance

Personal Data as per GDPR



Who is Data Principal ?

Data Principal refers to the individual whose data is being collected.

In the case of children (<18 years), their parents/lawful guardians will be considered their "Data Principals".

(a) Adult

(b) children

Figure: Data Principal

Who is Data Fiduciary ?

Meaning of fiduciary

Involving trust, especially with regard to the relationship between a trustee and a beneficiary.
Eg. "The company has a fiduciary duty to shareholders"

ഏകദേശ മലയാളം അർത്ഥം വിശ്വസ്ഥത വിശ്വാസത്തിൽ അധിഷ്ഠിതമായ രക്ഷാധികാരി എന്നൊക്കെ എടുക്കാം

Fiduciary

Sounds like

fuh·**dyoo**·shuh·ree

Who is Data Fiduciary ?

DPDP bill defines

"Data Fiduciary" as any **person** who alone or in conjunction with other persons determines the purpose and means of processing of personal data

Person includes

an individual;

a Hindu Undivided Family;

a company;

a firm;

an association of persons or a body of individuals, whether incorporated or not;

the State; and

every artificial juristic person

Who is Data processor and What is processing ?

Data Processor

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

Processing

in relation to personal data means an automated operation or set of operations performed on digital personal data, 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
- destruction

Gain, Harm and Loss

Gain

Gain in property or a supply of services, whether temporary or permanent; or

An opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration.

"harm", in relation to a Data Principal, means

-

Any bodily harm; or

Distortion or theft of identity; or

Harassment; or prevention of lawful gain or causation of significant loss;

loss" means –

Loss in property or interruption in supply of services, whether temporary or permanent; or

A loss of an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration

Issues with "harm"

The 2019 Bill recognized unambiguously that some harms require greater measures of protection and redressal mechanisms in place than others, which has been excluded from the present Bill

Application of the Act

The act apply to the processing of digital personal data within the territory of India where

- Such personal data is collected from Data Principals online; and
- Such personal data collected offline, is digitized.

Processing of digital personal data outside the territory of India, if such processing is in connection with any profiling of, or activity of offering goods or services to Data Principals within the territory of India.

Profiling = processing of personal data that analyses or predicts aspects concerning the behavior, attributes or interests of a Data Principal.

Act is not applicable

Non-automated processing of personal data;

Offline personal data;

Personal data processed by an individual for any personal or domestic purpose; and

Personal data about an individual that is contained in a record that has been in existence for at least 100 years.

Obligations of Data Fiduciary-Notice

Grounds for processing digital data.

Allowed to process data only for the lawful purpose for which consent is given or deemed to have been given

Comment lawful is somewhat vague. The purpose must be specific and clear

Obligations of Data Fiduciary -Notice

Issue itemized Notice to data principal

Itemized notice should be in clear and plain language

Description of personal data sought to be collected

Purpose of processing such personal data

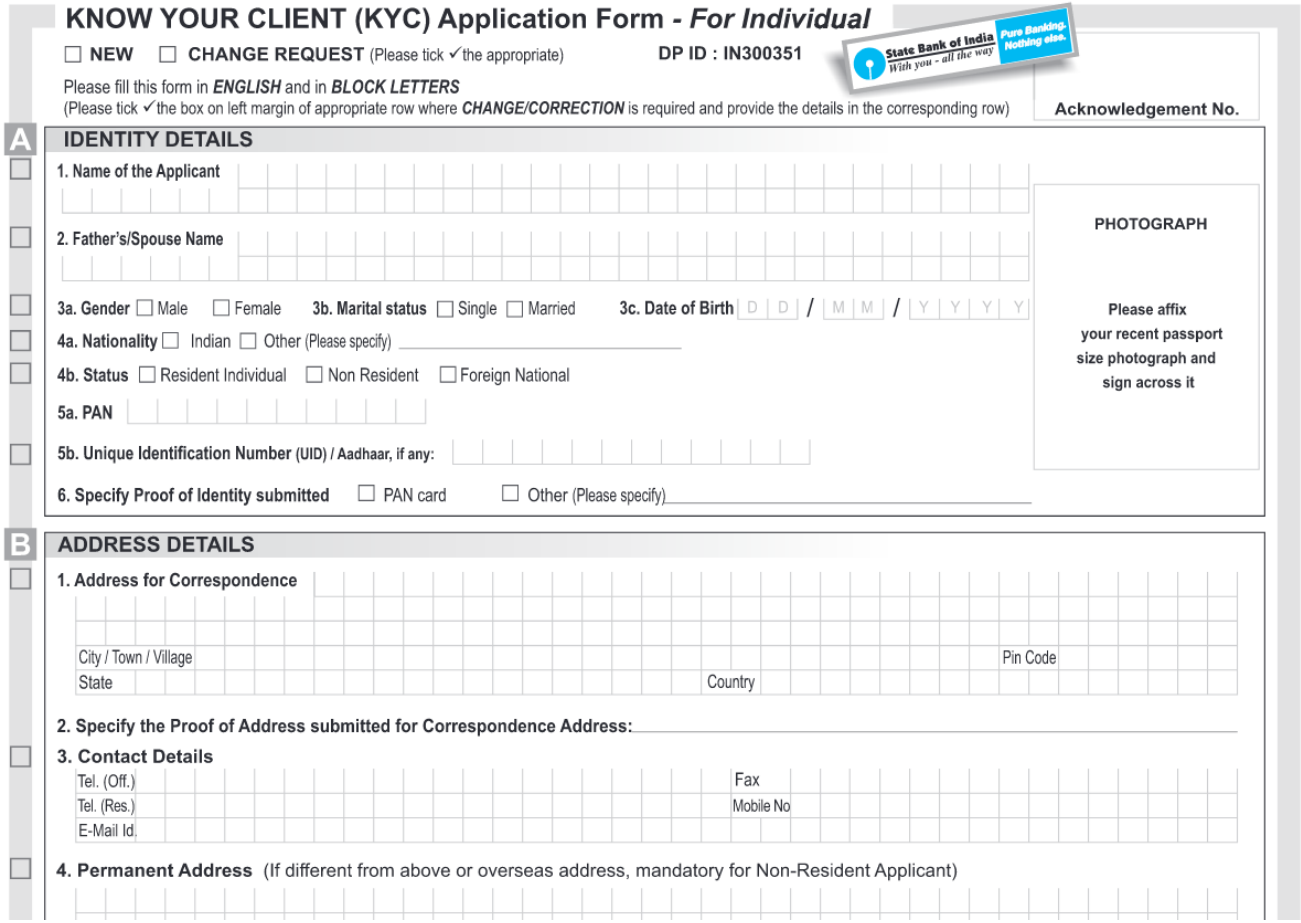
Notice

Can be a separate document, or an electronic form, or a part of the same document in or through which personal data is sought to be collected,

itemized

A list of individual items

Obligations of Data Fiduciary-Notice



KNOW YOUR CLIENT (KYC) Application Form - *For Individual*

☐ NEW ☐ CHANGE REQUEST (Please tick ✓the appropriate) DP ID : IN300351

State Bank of India — With you - all the way — Pure Banking. Nothing else.

Please fill this form in ***ENGLISH*** and in ***BLOCK LETTERS***

(Please tick ✓the box on left margin of appropriate row where ***CHANGE/CORRECTION*** is required and provide the details in the corresponding row)

Acknowledgement No.

A IDENTITY DETAILS

1. Name of the Applicant

2. Father's/Spouse Name

PHOTOGRAPH

Please affix your recent passport size photograph and sign across it

3a. Gender ☐ Male ☐ Female 3b. Marital status ☐ Single ☐ Married 3c. Date of Birth D D / M M / Y Y Y Y

4a. Nationality ☐ Indian ☐ Other (Please specify) _____

4b. Status ☐ Resident Individual ☐ Non Resident ☐ Foreign National

5a. PAN

5b. Unique Identification Number (UID) / Aadhaar, if any:

6. Specify Proof of Identity submitted ☐ PAN card ☐ Other (Please specify) _____

B ADDRESS DETAILS

1. Address for Correspondence

City / Town / Village Pin Code

State Country

2. Specify the Proof of Address submitted for Correspondence Address: _____

3. Contact Details

Tel. (Off.) Fax

Tel. (Res.) Mobile No

E-Mail Id

4. Permanent Address (If different from above or overseas address, mandatory for Non-Resident Applicant)

Before collecting these information bank should give you a notice stating the purpose.

Obligations of Data Fiduciary-Consent

Consent of the Data Principal

freely given,

specific,

informed and unambiguous

indication of the Data Principal's wishes to the processing of her personal data for the specified purpose.

Obligations of Data Fiduciary-Consent

Request for consent

- Should be Clear and in plain language ,
- Details of a data protection officer or responsible individual should be given
- Data principal has the option to access the request in any language listed in 8th schedule of the constitution

Obligations of Data Fiduciary-Consent

Data Principal has the Right to withdraw consent

- At any time
- The consequences of such withdrawal shall be borne by such Data Principal
- Up on withdrawal Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing of the personal data

Consent Manager

Consent Manager

The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.

The Consent Manager specified in this section shall be an entity that is accountable to the Data Principal and acts on behalf of the Data Principal

Obligations of Data Fiduciary-Questions on Consent

Burden of Proof

Data Fiduciary shall be obliged to prove that a notice was given by the Data Fiduciary to the Data Principal and consent was given by the Data Principal

Deemed consent

A Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary

- Reasonable expectation eg. Number taken for reservation
- For the performance of any function under any law by state eg bank account no for crediting a refund
- For compliance with any judgment or order issued under any law;
- For responding to a medical emergency
- To provide medical treatment or health services to any individual during an epidemic
- 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
- In public interest

Please refer to the draft bill for details

General obligations of Data Fiduciary

A Data Fiduciary shall be responsible for complying with the provisions of this Act

Data Fiduciary shall make reasonable efforts to ensure that personal data processed by or on behalf of the Data Fiduciary is accurate and complete, if the data is used for

- making decisions that affect data principal
- is likely to be disclosed by the Data Fiduciary to another Data Fiduciary

Implement appropriate technical and organizational measures

Take reasonable security safeguards to prevent personal data breach.

In the event of a personal data breach, the Data Fiduciary or Data Processor as the case may be, shall notify the Board and each affected Data Principal,

A Data Fiduciary must cease to retain personal data as soon as the purpose is over or the legal or business necessity is over

Publish details of data protection officer

Set up a grievance redressal mechanism

Transfer data to another data fiduciary or data processor only with a valid contract

Obligations: personal data of children

A data fiduciary should

- Obtain Parent consent
- Not permitted to do tracking or behavioral monitoring
- Not undertake such processing of personal data that is likely to cause harm to a child

Significant Data Fiduciary

The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of relevant factors, including:

(a) the volume and sensitivity of personal data processed;

(b) risk of harm to the Data Principal;

(c) potential impact on the sovereignty and integrity of India;

(d) risk to electoral democracy;

(e) security of the State;

(f) public order; and

(g) such other factors as it may consider necessary;

Obligations of Significant Data Fiduciary

Appoint Data protection officer

Appoint data auditor to evaluate compliance of the act

Undertake such other measures including Data Protection Impact Assessment

Comment : While the present Bill does recognise 'significant data fiduciaries', it defers to the Government to lay out the grounds for defining them through Rules which the Government can introduce at a later date. Such an omission and deference concentrates the power with the Executive, and delegates a function which belongs within the remit of the legislature

Rights of Data Principal

Right to information about personal data

The Data Principal shall have the right to obtain from the Data Fiduciary:

(1) the confirmation whether the Data Fiduciary is processing or has processed personal data of the Data Principal;

(2) a summary of the personal data of the Data Principal being processed or that has been processed by the Data Fiduciary and the processing activities undertaken by the Data Fiduciary with respect to the personal data of the Data Principal;

(3) in one place, the identities of all the Data Fiduciaries with whom the personal data has been shared along with the categories of personal data so shared; and

(4) any other information as may be prescribed.

Rights of Data Principal

Right to correction and erasure of personal data

A Data Principal shall have the right to correction and erasure of her personal data, in accordance with the applicable laws and in such manner as may be prescribed.

A Data Fiduciary shall, upon receiving a request for such correction and erasure from a Data Principal:

(a) correct a Data Principal's inaccurate or misleading personal data;

(b) complete a Data Principal's incomplete personal data;

(c) update a Data Principal's personal data;

(d) erase the personal data of a Data Principal that is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose.

Rights of Data Principal

Right of grievance redressal

Register a complaint with data fiduciary

Approach Data protection board

Right to nominate

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.

For the purpose of this section, "incapacity" means inability to exercise the rights of the Data Principal under the provisions of this Act due to unsoundness of mind or body.

Duties of Data Principal

A Data Principal shall comply with the provisions of all applicable laws while exercising rights under the provisions of this Act.

A Data Principal shall not register a false or frivolous grievance or complaint with a Data Fiduciary or the Board.

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.

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.

Transfer of Data outside India

The Central Government may notify such countries or territories outside India to which a Data Fiduciary may transfer personal data

Exemptions

The provisions of Chapter 2 (OBLIGATIONS OF DATA FIDUCIARY) except sub-section (4) of section 9 (not clear) , Chapter 3 (rights and duties of data principal) and Section 17 (transfer beyond border)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.

Government Exemptions

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.

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.

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.

Government Exemptions: issues

Section 18 of the Bill has widened the scope of government exemptions even further. The requirement of proportionality, reasonableness and fairness have been removed for the Central Government to exempt any department or instrumentality from the ambit of the Bill.

This is in conflict with the law laid down in the K.S. Puttaswamy judgement1. The Supreme Court had explicitly held that the restriction on the right to privacy of an individual must withstand the test of proportionality.] The exemptions extended to the Government under the Bill cannot be said to meet these requirements.

Furthermore, the Bill's express exemption to the Government from deleting the data which it has collected despite the purpose of such data collection having been met contradicts the principles of purpose limitation, and data minimisation.

Compliance framework

Data Protection Board of India

- Statutes relating to the composition of the board is currently vague in the draft bill
- It will be appointed by central government
- Members will have the status of public servant (IPC section 21)

Compliance framework

Functions of Data protection Board of India

- to determine non-compliance with provisions of the Act and impose penalty under the provisions of the Act;
- to perform such functions as the Central Government may assign to the Board under the provisions of this Act or under any other law by an order published in the Official Gazette.

Standard legal principles such as "Audi alteram partem" should be followed.
Board will have the powers of a civil court.

Compliance framework

Review and Appeal

The Board may review its order

An appeal against any order of the Board shall lie to the High Court.

No other civil court will have jurisdiction in data privacy matters of persons.

Alternate Dispute resolution

The board can direct for alternate dispute resolution

Comment: The appeal jurisdiction is rather vague. It does not specify the jurisdiction of High courts.

Financial Penalty

Maximum 500 crores

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

Financial Penalty

While determining the amount of a financial penalty to be imposed under sub-section (1), the Board shall have regard to the following matters:

(a) the nature, gravity and duration of the non-compliance;

(b) the type and nature of the personal data affected by the non-compliance;

(c) repetitive nature of the non-compliance;

(d) whether the person, as a result of the non-compliance, has realized a gain or avoided any loss;

(e) whether the person took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action;

(f) whether the financial penalty to be imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with the provisions of this Act; and

(g) the likely impact of the imposition of the financial penalty on the person.

Clarifications Required

1. Lawful, Transparent and Fair usage of personal data by organisations.

2. Purpose Limitation - data is utilised only for the purpose for which it was collected in the first place.

3. Data Minimization – only that data which is required is collected, and not more.

4. Accuracy of personal data – updated and accurate personal data is stored by organisations.

5. Storage limitation – personal data is not stored beyond the time period for which it is actually required.

6. Security safeguards – adequate security measures to be in-place to prevent data breaches, unauthorised access, etc.

7. Accountability measures – holding the data fiduciary accountable for the processing of the data.

Thank You

References : Software Freedom Law Center, India