

Digital Data Protection Bill 2022

Explained

Dr. Sunil T T

College of Engineering Attingal

suniltt@gmail.com

December 12, 2022

Background: Global Scenario

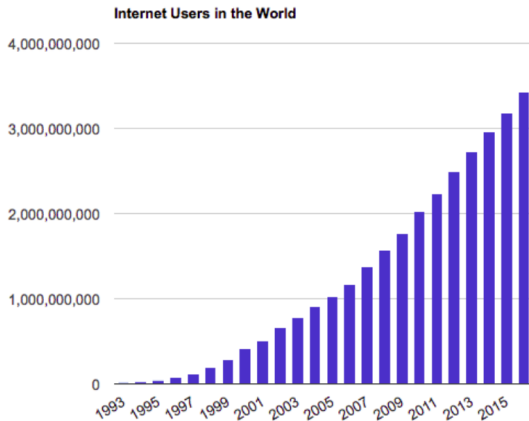
Growth of Internet

Major Data Breaches

Need for data protection

GDPR, US and Chinese laws

Background: Growth of Internet



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)

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 localisation 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 Localisation: Alleged blanket exception 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

Personal Data Breach

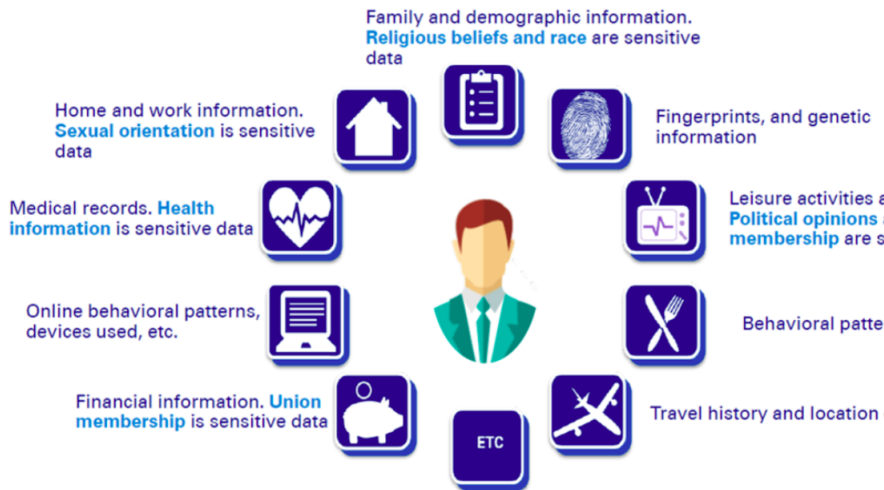
Any unauthorised

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.

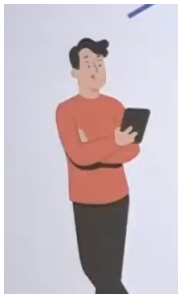
Personal Data as per GDPR



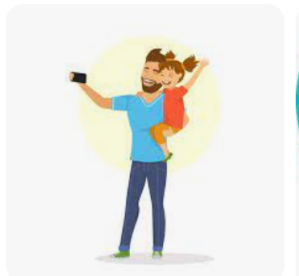
Who is Data Principal ?

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 വിശ്വസ്ത 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

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 behaviour, 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

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

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

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

☐ 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)

PHOTOGRAPH

Please affix your recent passport size photograph and sign across it

B ADDRESS DETAILS

☐ 1. Address for Correspondence

City / Town / Village
State Country Pin Code

☐ 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

Obligations of Data Fiduciary-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

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 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.