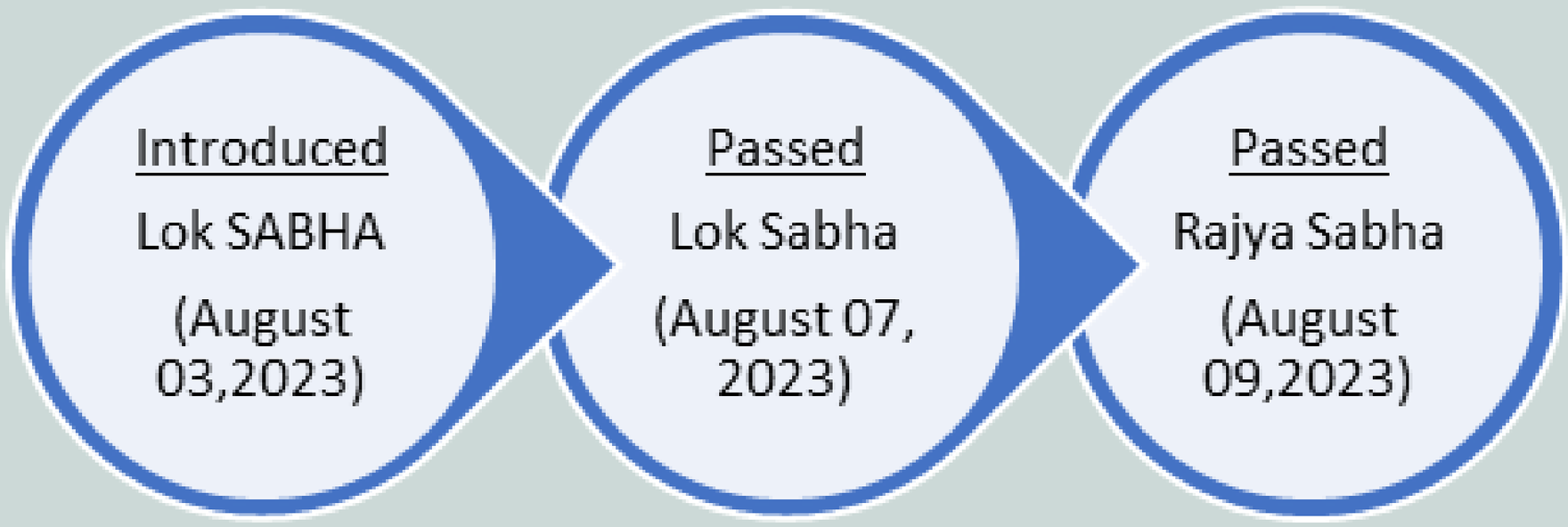
DIGITAL PERSONAL DATA PROTECTION ACT 2023 OVERVIEW: FAQS TO THE RESCUE!

Wednesday Wisdom
23-08-2023

Images taken from public sources for the academic purpose

A Timeline indicating the stages the Bill went through until the formation of The Digital Data Protection Act, 2023 (Act)

TIMELINE	STAGES
July 2017	**Ministry of Electronics and Information Technology constituted an expert committee under the chairmanship of Justice BN Sri Krishna**
August 2017	**K.S. Puttaswamy (Retd.) vs. Union of India[2] (Puttuswamy Case) was passed that not only solidified the right to privacy as a fundamental right but also catalyzed efforts to establish a comprehensive data protection regime in India**
July 2018	**Ministry of Electronics and Information Technology released BN Srikrishna Committee report and proposed draft bill.**
December 2019	**Revised Personal data protection bill was introduced in Lok Sabha.**
December 2021	**Joint Parliamentary Committee submitted its reports along with a new draft bill -Personal Data Protection Bill 2021**
August 2022	**The Indian Government withdrew the Bill from Lok Sabha**
Nov 2022	**Ministry of Electronics and Information Technology releases a fresh new draft Bill called Digital Personal Data Protection (DPDP) bill, 2022 for public poll consultation.**



[1] The article reflects the general work of the authors and the views expressed are personal. No reader should act on any statement contained herein without seeking detailed professional advice.
[2] Writ Petition (Civil) No 494 of 2012

Digital Personal Data Protection Bill received the President's assent on 11th August 2023 and was published in Official Gazette on 12th August 2023.

Q1: What is the purpose of enacting Digital Personal Data Protection Act 2023 ("Act")?

The Digital Data Protection Act 2023 has been enacted as a legislative framework aimed at safeguarding the privacy and security of digital personal data belonging to individuals and other entities like HUF, company, firm or an association of persons (Person). It establishes guidelines for collecting, processing, storing, and sharing digital data.

Q2. How did the Supreme Court's decision in the Puttaswamy case impact data protection in India?

The case revolved around the constitutional validity of the Aadhaar project, a biometric identification system used in India. The judgment, delivered on August 24, 2017, by a Nine judge bench of the Apex Court, established the right to privacy as a fundamental right under the Indian Constitution under Article 19 and 21 and set the platform for comprehensive data protection regulations in the country. The judgement also catalyzed efforts to establish a comprehensive data protection regime in India, bringing the country's data protection practices in line with global standards.

Images taken from public sources for the academic purpose

Q3: What is the Scope of Application of the Act?

The Act defines digital personal data and aims to regulate all processing of such digital personal data and imposes penalties for any unauthorized personal data breach or unauthorized processing or misuse of such data.
The Act also provides for duties on Data Principals and Data Fiduciaries (elaborated hereinbelow).

Q4: Does the Act apply to digital personal data processed outside the territory of India?

Yes, the Act also applies to the digital personal data processed outside the territory of India if it is processed in connection to the goods or services provided to Data Principals in India.

Q5: What does the Act exclude?

The Act excludes:
a)Processing of any personal data by an individual for personal or domestic purposes;
b)Any disclosures that are made voluntarily by any individual.
c)Any disclosure by a person who was required to make such disclosure under any legal obligation.

Example as provided in the Act: X, an individual, while blogging her views, has publicly made available her personal data on social media. In such a case, the provisions of this Act shall not apply.

Q6: How does the Act deal with concept of Personal Data and Digital Personal Data?

Personal data is defined as any data stating identity of an Individual or who is identifiable by or in relation to such data.

Examples: Person's name, address, phone number, email address, and date of birth.

Digital Personal Data: Any kind of Personal data specifically in Digital Form. It can be in the form of Online accounts data (includes usernames, passwords, and profile associated with online services), Browsing and Search History, Location data, Cookies and tracking data, Transactional data (online purchases, information about health tracking devices, Biometric data, etc.

The Act shall also apply to data that is collected in non-digital format and digitized subsequently. It does not cover non-digital personal data and non-personal data.

Q7: Who acts as the Data Principal?

A "Data Principal" is a term used in the Act to refer to an individual to whom personal data relates. In the context of data protection regulations, the data principal is the person about whom the personal data is collected, processed, or stored.

Data Principals have rights over their personal data such as

- Right to Correction and Erasure of such data ;
- Right to grievance redressal in respect of any data breach;
- Right to have access to their process data;
- Right to nominate any individual who shall be entitled to exercise their rights in the event of death or any incapacity of the data principal;
- Right to withdraw their consent and in case of such withdrawal, the data fiduciary shall not be entitled to process the data further;

Data Principals also have the following obligations:

- Comply with the provisions of all applicable laws while exercising rights under this Act;
- Not to impersonate any other person while providing personal data;
- Not to suppress any material information as to personal data;
- Not to lodge any false or frivolous complaint with Data Fiduciary or Board ;
- To submit authentic information while exercising Right of correction or erasure ;

Example: There is an online shopping website called "Chainmart." Users can create accounts on the website, buy products and make purchases while providing various types of personal information during the shopping process. The online users using the “Chainmart” platform are the Data Principals. They have ownership and control over their personal data, and the platform is obligated to handle their data responsibly, provide transparency about data processing practices.

Q8: Who is Data Fiduciary?

A Data Fiduciary is a term used in the Act to refer to an entity or individual that collects, processes, and controls personal data on behalf of another individual, known as the Data Principal. The data fiduciary is expected to act in the best interests of the data subjects and take appropriate measures to protect their privacy and rights.

To take forward the earlier example, Chainmart collects and uses data of users including names, email addresses, cart list, reviews, comments etc. “Chainmart” as the platform that collects, stores, and processes users’ personal data, acts as the Data Fiduciary.

Q9: What Obligations are to be followed by Data Fiduciaries while collecting data?

Data fiduciaries are required to ensure that:

- any processing is also properly consented for certain legitimate use or purpose by the data Principals;
- while seeking consent from the data principal, the contact details of a Data Protection Officer or any other person for contact should be mentioned.
- If at any stage, any of the process is challenged in Courts, the proof of burden will lie with the Data Fiduciary to prove that consent was obtained for processing personal data.
- The purpose needs to be defined clearly and it should have a direct proximity with the data collected.

Example as provided in the Act: X, an individual, downloads Y, a telemedicine app. Y requests the consent of X for (i) the processing of her personal data for making available telemedicine services, and (ii) accessing her mobile phone contact list, and X signifies her consent to both. Since phone contact list is not necessary for making available telemedicine services, her consent shall be limited to the processing of her personal data for making available telemedicine services.

There are additional safeguards imposed while collecting data from minors and persons with disabilities.

There are also certain cases where consent is not required, where the data will be used for “legitimate purpose”, like:

a. Data provided voluntarily by the Data Principal to the Data Fiduciary;
b. In case of medical emergency where it involves threat to life;
c. In the case of employment, any reasons related to employment and to safeguard employer from any kind of corporate espionage, threat of trade secrets being stolen, where a Data Principal is an employee.

Q10: What is a Consent, how is it obtained & can it be withdrawn?

Consent is not defined in the Act but generally it is understood that two or more persons are said to have consent when they agree upon the same thing in the same sense.

To obtain consent under the Act, Data Fiduciary must ensure that any kind of request made towards Data Principal for obtaining consent shall be accompanied or preceded by a Notice informing or alerting the Data Principal about

1. the personal data and the purpose for which the data collection is to be processed.
2. the rights that the Data Principal will be having after giving consent and;
3. the modes Data Principal must be having for making any complaint to the respective Data Protection Board (“Board”)established by Central Government under the Act.

<u>Let us understand this through an example:</u>
X, an individual, opens a bank account using the mobile app or website of Y, a bank. To complete the Know-Your-Customer requirements under law for opening of bank account, X opts for processing of her personal data by Y in a live, video-based customer identification process. Y shall accompany or precede the request for the personal data with notice to X, describing the personal data and the purpose of its processing.

Here X is the Data Principal and Y is the Data Fiduciary and the consent is limited to the purpose of completing KYC for opening a bank account. The bank shall not be entitled to process the data for any other purpose.

The general requirements of free specific, informed, and unconditional consent from the parties are applicable to the consent under data protection regime as well. One must note that personal data collected or shared will be for specified purposes only and processing can thus, be limited only for such specified purposes.

The Data Principals have been handed with a right for the Withdrawal of consent at any point of time. The Data Fiduciary is required to stop providing the services relating to the processing of personal data once the consent is withdrawn, subject to certain exceptions under the Act.

Q11: What are the exemptions under this Act?

- Processing personal data which is required to uphold legal rights or make legal claims.
- Personal data can be used by courts, tribunals, or other authorized bodies in India to carry out tasks related to law, judgment, oversight, or regulation. This use is essential for these functions to be fulfilled.
- Personal data is handled to stop, find, look into, or take legal action against any wrongdoing or violation of current laws in India.
- If person in India has an agreement with a Data Principal outside India, they can use personal data of individuals who are not in India as part of that agreement.
- The processing of personal data is necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies.
- For determining the financial situation of a person who has defaulted on loan.

Example: X, an individual, takes a loan from Y, a bank. X defaults in paying her monthly loan repayment instalment on the date on which it falls due. Y may process the personal data of X for ascertaining her financial information and assets and liabilities.

Q12: What kind of Penalties can be imposed upon any violation or any breach?

The Act imposes significant penalties for any breaches and violations:

- Penalty on Data fiduciaries for failure to take reasonable security safeguards to prevent personal data breach: Up to ₹250 crores.
- Penalty on Data fiduciaries for failure to notify the Board and affected Data Principals of a personal data breach: Up to ₹200 crores.
- Penalty on Data Fiduciaries for breach in observance of any additional obligations with respect to personal data of children.
- Penalty on Data principals for violation of duties as mentioned in the Act: Up to ₹10,000.
- Penalty for Breach of any term of voluntary undertaking accepted by the Board: Penalty up to the extent applicable for the breach in respect of which the proceedings against the entity were instituted.
- Penalty for any other breaches of this Act: Up to ₹50 crores.

Q13: What are the new key compliances under the Act as compared to the previous legislation for Data Fiduciaries?

Data Fiduciaries must adhere to all the duties as laid down in the Act. Though there are no timelines for immediate implementation, the Act lays down certain specific adherences by Data Fiduciaries:

a) The Data Fiduciary must obtain consent clearly and also send a proper notice informing the Data Principal about the:

- reason, purpose, and the means for which Data is processed.
- The right to withdraw her consent at any time.
- The manner in which a complaint can be made to the Board

As per an illustration in the Act:

X, an individual, gave her consent to the processing of her personal data for an online shopping app or website operated by Y, an e-commerce service provider, before the commencement of this Act. Upon commencement of the Act, Y shall, as soon as practicable, give through email, in-app notification or other effective method information to X, describing the personal data and the purpose of its processing.

b) Data fiduciaries are required to appoint a Single Point of Contact termed as Consent Manager, who generally collects, reviews or manages Consent requests placed by Data Principals towards Data Fiduciaries. These Consent Managers should be registered with the respective Data Protection Board.

c) The Act requires Data Fiduciaries to get permission from parents and legal guardians in a provable way before handling personal data of children (those under 18 years old) and individuals with disabilities.

d) The Act obliges the Data Fiduciary or Data Principal to notify the respective Board of data breaches.

Images taken from public sources for the academic purpose

Q 14. What is the mechanism suggested in the Act to adjudicate data breaches?

The Act mandates the government to create an Independent Data Protection Board (Board) which shall serve as the sole adjudicating body for any disputes related to personal data breaches or any violations under the Act. Jurisdiction of civil courts is specifically ousted under the Act. The Board shall have all the powers, of the civil court:

1. to conduct inquiries and Investigations and to impose penalties under the Act.
2. To review complaints filed by Data Principals in respect of breach by Consent Manager or Data Fiduciary;
3. To Receive complaints, conduct hearings, make judgments, and perform other related tasks.
4. To refer parties to mediation, if so deemed fit by the Board.
5. The Board can also imposed penalties upon the complainant if it finds at any stage that the filed complaint is of false or frivolous nature.

Any Person aggrieved by any order of the Board shall be entitled to file an appeal before the Appellate Tribunal within a period of 60 (sixty) days of the order.

Images taken from public sources for the academic purpose

For any feedback or response on this article, the author can be reached on pranav.mane@ynzgroup.co.in and priya.shahdeo@ynzgroup.co.in

Author: Pranav Mane

Pranav is an Associate at YNZ Legal. By qualification he is Bachelor of commerce and Bachelor of Law from Mumbai University. He is also a member of Bar Council of Maharashtra and Goa

Co-author: Priya Shahdeo

Priya is a Manager-Corporate at YNZ Legal. By qualification she has completed her Bachelor of Arts and Bachelor of Law from Bharati Vidyapeeth Deemed University.

Images taken from public sources for the academic purpose