Newsflash
Key Aspects of The Digital Personal Data Protection Act, 2023

THE POWER OF BEING UNDERSTOOD

RSM

Newsflash

Key Aspects of The Digital Personal Data Protection Act, 2023

For Circulation

14 August 2023

1.0 Introduction

Currently, India with over 80 crore internet users is amongst the highest consumers and producers of data per capita amongst the countries. Digital India has transformed the lives of crores of Indians. With this, personal data security and privacy issues have become very important aspects of our daily interactions and have thus figured prominently across various forums in recent years. On 24th August 2017, a nine Judge Bench of the Supreme Court delivered a unanimous verdict in ***Justice K.S. Puttaswamy vs. Union of India*** and other connected matters, affirming that the Constitution of India guarantees to each individual a fundamental right to privacy.

Against this backdrop, it became important to have a law to address the privacy of data. Brief timelines of the Bill are as follows:

Year	Particulars
August 2018	SriKrishna Committee submitted a draft report to IT Ministry highlighting the inadequacies of IT Rules, 2011
December 2019	The Personal Data Protection Bill, 2019 was introduced in Lok Sabha
December 2021	Data Protection Bill 2021 tabled in the parliament
August 2022	Data Protection Bill 2021 withdrawn
November 2022	Draft Personal Data Protection Bill, 2022 released for public consultation
August 2023	The President of India has granted her assent to The Digital Personal Data Protection Bill, 2023 on Friday, August 11, 2023. The Bill was passed unanimously by the Rajya Sabha on August 9 while the Lok Sabha passed the bill on August 7 by a voice-vote.

2.0 Highlights of the Digital Personal Data Protection Act, 2023 ('Act')

The said Act, inter alia, seeks—

(a) to provide for the protection of digital personal data;
(b) to lay down grounds for processing personal data;
(c) to place general and in certain cases special obligations on entities that process personal data;
(d) to confer certain rights in respect of their personal data on individuals;
(e) to provide for duties to be performed by individuals while exercising their rights and providing their personal data for certain purposes;

(f) to lay down a digital by design compliance framework for easy and faster implementation of the proposed Legislation;
(g) to enable parties to a dispute to attempt resolution of the dispute through alternate process and person of their choice;
(h) to provide monetary penalties for lapses and non-compliance of the provisions of the proposed Legislation; and
(i) to enable voluntary undertaking to encourage faster resolution and rectification of lapses.

The provisions of this Act shall be in addition to and not in derogation of any other law for the time being in force. In the event of any conflict between a provision of this Act and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict.

3.0 Use of Personal data:

The regulations allow the use of personal data for the following purposes only in accordance with the provisions of the Act and for a lawful purpose:

a. for which consent is given by the Data Principal; or
b. for certain legitimate uses.

4.0 Applicability:

This Act would apply to personal data **collected in India** whether in digital form or collected in non-digital form and digitized subsequently, personal data **processed outside India for offering goods or services to Data Principals within the territory of India.**

The provisions of this Act will **not be applicable** in the case of personal data processed by an individual for **personal or domestic purposes** and personal data made **publicly available** by the Data Principal or by any other person **pursuant to a legal obligation**.

Illustration:

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.

5.0 Some important definitions:

5.1 Consent Manager:

A person registered with the Data Protection Board ('the Board') who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw her consent through an accessible, transparent, and interoperable platform.

Rules regarding the manner of accountability and the obligations of consent manager and the manner of registration of Consent Manager and the conditions relating thereto are yet to be notified.

5.2 Data Fiduciary:

Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

5.3 Data Principal:

The individual to whom the personal data relates and where such individual is-

i. a child, includes the parents or lawful guardian of such a child.
ii. a person with disability, includes her lawful guardian, acting on her behalf.

5.4 Data Processor:

Any person who processes personal data on behalf of a Data Fiduciary.

5.5 Data Protection Officer:

An individual appointed as such by a Significant Data Fiduciary under the provisions of this Act.

5.6 Personal data:

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

5.7 Personal data breach:

Any unauthorized 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.

5.8 Person

Person includes an individual, a Hindu Undivided Family, a Company, a firm, an association of persons or body of individuals, whether incorporated or not, the State and every artificial juristic person, not falling within any of the preceding sub-clauses.

5.9 Processing:

Processing in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organization, structuring, storage, adaptation, retrieval, use, alignment, or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure, or destruction.

5.10 Significant Data Fiduciary

means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10.

6.0 Key Aspects:

6.1 A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and Rules made thereunder and for a lawful purpose.

6.2 Consent management:

a. On or before requesting a Data Principal for consent, a Data Fiduciary shall give to the Data Principal an itemized notice (in English or any language specified in Eight Schedule to the Constitution) of the personal data sought and the reason.

b. Consent given by the Data Principal for such data shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action.

c. Data Principal may give, manage, review, or withdraw consent to the Data Fiduciary.

d. Consent will not be required for 'legitimate uses' such as

   (i) specified purpose for which data has been provided by an individual voluntarily to the Data Fiduciary,

   (ii) provision of benefit or service by the government,

   (iii) medical emergency, and

   (iv) employment.

e. Processing data of child and person with disability who has a lawful guardian, must be done only with the verifiable consent of parent/ lawful guardian.

Illustration:
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.

Illustration on legitimate use for specified purposes:
X, an individual, makes a purchase at Y, a pharmacy. She voluntarily provides Y her personal data and requests Y to acknowledge receipt of the payment made for the purchase by sending a message to her mobile phone. Y may process the personal data of X for the purpose of sending the receipt.

6.3 Obligations of Data fiduciary:

A Data Fiduciary shall:

a. at all times be responsible for complying with the provisions of this Act by ensuring that all appropriate organizational and technical measures are in place.

b. in the event of a personal data breach, the Data Fiduciary shall notify the Board and each affected Data Principal.

c. appoint and publish business contact information of a Data Protection Officer (DPO), wherever applicable.

d. build reasonable security safeguards to prevent a data breach,

e. erase personal data as soon as the purpose has been met and retention is not necessary for legal purposes (storage limitation).

f. Firms dealing with user data must protect such data, even if stored with a third-party processor.

g. establish an effective mechanism to redress the grievances of Data Principals.

Illustration for erasing personal data:

X, an individual, registers herself on an online marketplace operated by Y, an e-commerce service provider. X gives her consent to Y for the processing of her personal data for selling her used car. The online marketplace helps conclude the sale. Y shall no longer retain her personal data.

6.4 Rights and Duties of Data Principal:

The Data Principal has various rights like

a. the right to access information about her personal data used for data processing,
b. correction and erasure of personal data, of grievance redressal,
c. to nominate another person to exercise rights in case of death or incapacity.

Duties of Data Principal:

a. comply with the provisions of all applicable laws;
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;
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.

6.5 Transfer of Data outside India:

Transfer of personal data outside India is allowed except to countries restricted by Central Government as may be notified.

6.6 Data Protection Board:

a. Establishment of Data Protection Board of India by the Central Government. Apart from other aspects, the Board will analyze non-compliance with this Act and impose penalties depending upon the nature, impact, and gravity of the breach.

b. Appeals can be made in the Appellate Tribunal (i.e., the Telecom Disputes Settlement and Appellate Tribunal) against DPB decisions.

6.7 Registration of Consent Manager:

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.

6.8 Significant Data Fiduciary (SDF):

The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, based on 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.

6.9 Obligations of SDF:

a. Appointment of a Data Protection Officer
b. Appointment of an independent data auditor to carry out data audit;
c. Periodic Data Protection Impact Assessment; and
d. Periodic audit.

6.10 Penalties:

Sr. No.	Breach of provisions of this Act or rules made there under	Penalty
1.	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under section 8(5).	May extend to Rs. 250 crores
2.	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under section 8(6).	May extend to Rs. 200 crores
3.	Breach in observance of additional obligations in relation to children under section 9.	May extend to Rs. 200 crores
4.	Breach in observance of additional obligations of Significant Data Fiduciary under section 10.	May extend to Rs. 150 crores

5.	Breach in observance of the duties under section 15.	May extend to Rs. 10,000
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 was instituted.
7.	Breach of any other provision of this Act or the rules made thereunder	May extend to Rs. 50 crores

7.0 Impact and Way Forward

The Rules relating to technical and organisational measures to be adopted by a Data Fiduciary are yet to be notified. The Board seems to be having a significant role in the implementation of the Act, including registration of the Consent Manager, determination of penalty in the event of breach and other administrative matters. Once the Rules are formulated and the Board is constituted, there will be further clarity on the implications arising out of the Data Protection Regulations in India.

Further, the Act states that consent is not required for legitimate use of the data shared voluntarily by the individual for specific purposes. However, clarity may be required on the nature of legitimate use, for instance, prospective client sharing visiting cards which is digitized and stored in organization's database.

The Act is anticipated to build trust between customers and businesses by giving the former more protection and control over their personal data. This may result in better communication between businesses, their stakeholders, and customers.

The Act can promote wider adoption of digital technologies by increasing customer confidence in digital goods and services by guaranteeing personal data protection. This will help businesses flourish better in the Indian market.

While this Act is likely to have a magnanimous impact on various industries including telecommunication, healthcare, banking, and financial and e-commerce companies, etc., data fiduciaries and data processors will have to:

- make huge investments in new technologies and processes for processing data securely;
- sensitise workforce/merchants/vendors/customers, in handling/sharing of personal data;
- enterprises based outside India serving individuals in India, will also need systems and processes to adhere to the Act.
- Enterprises will have to review their current ways of working especially on the personal data front such as their employees, customers, merchants, vendors, etc. to be able to honor the rights that individuals may exercise, such as the right to access, update, erase their data, etc.

For further information please contact:

RSM Astute Consulting Pvt. Ltd.

8th Floor, Bakhtawar, 229, Nariman Point, Mumbai - 400021.

T: (91-22) 6108 5555/ 6121 4444
F: (91-22) 6108 5556/ 2287 5771

E: emails@rsmindia.in

W: www.rsmindia.in

Offices: Mumbai, New Delhi - NCR, Chennai, Kolkata, Bengaluru, Surat, Hyderabad, Ahmedabad, Pune, Gandhidham, Jaipur and Vijayanagar.


facebook.com/RSMinIndia


twitter.com/RSM_India


linkedin.com/company/rsm-india


Youtube.com/c/RSMIndia

This Newsflash summarizes on the key aspects of The Digital Personal Data Protection Act, 2023**.** It may be noted that nothing contained in this newsflash should be regarded as our opinion and facts of each case will need to be analyzed to ascertain applicability or otherwise of the said judgement and appropriate professional advice should be sought for applicability of legal provisions based on specific facts. We are not responsible for any liability arising from any statements or errors contained in this newsflash.

14 August 2023