ICRIER PROSUS
CENTRE FOR INTERNET AND DIGITAL ECONOMY

EVOLUTION OF INDIA'S **DATA PROTECTION** LAW: A PRIMER

POLICY BRIEF
4

AUGUST 2023

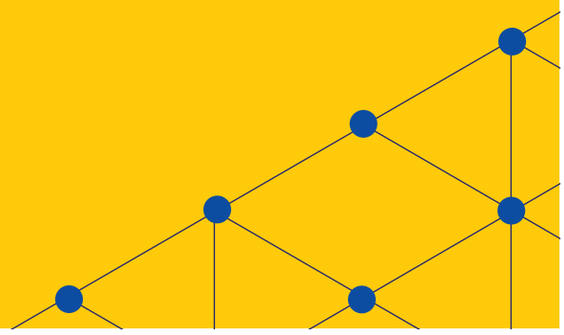
Abstract

This policy brief is intended as a primer on the evolution of India's data protection law. It briefly recounts how the law was developed through different drafts and consultations. It also provides a comparison of different versions of the law on its overall remit as well as provisions for data breaches, right to be forgotten, right to data portability, data localisation, exempted parties, impact assessment, institutional framework, harms, compensation and penalties. We find that the current version of the Digital Data Protection Act, 2023 has changed track on various provisions when compared to previous iterations.

Prepared by Shiva Kanwar and Mayank Manish

Authors' email: skanwar@icrier.res.in, mmanish@icrier.res.in

.



CONTENTS

List of Figure and Table

Evolution of India's Data Protection Law: A Primer

Introduction

The omnipresent internet has resulted in a data-driven world. People use the internet for work, education, payments, entertainment and access to government services resulting in exchange of personal data on a massive scale. The need for protection from misuse of personal data is therefore imperative. Broadly, a data protection law aims to ensure that every individual's data is secure, used fairly, and treated ethically and appropriately. It gives individuals more control over their data including the ability to access and provide consent for use. It establishes accountability for those processing data, and includes adequate redressal mechanisms in case of harm.

After years of deliberations and consultations, and multiple attempts at legislation, India has enacted a data protection law. The following section delineates India's efforts to enact a data protection legislation.

India's Data Protection Law: A Timeline

In 2011, the erstwhile Planning Commission established an Expert Committee on Privacy under the Chairmanship of Justice A.P. Shah to 'study privacy laws in various countries, identify privacy issues, and prepare a report with specific suggestions to facilitate authoring of the Privacy bill'.[1] The committee released its report in 2012 and recommended the creation of an overarching law for privacy protection based on five salient features:[2] (i) Technological neutrality and inter-operability with international standards, (ii) Multi-dimensional privacy, (iii) Horizontal applicability, (iv) Conformity with privacy principles, and (v) Co-regulatory enforcement regime.

The report also featured nine national privacy principles central to the interpretation of the right to privacy. These national privacy principles were intended to establish safeguards and procedures for processing of data, as well as establish rights of the people in relation to their data. Intended to be the cornerstone for privacy legislation, the principles are:[3]

1. Notice: during data collection and in other cases such as data breaches
2. Choice and Consent: individuals to be given choices with regard to providing their personal information, withdrawal of consent
3. Collection Limitation: only collect information that is necessary for the purpose
4. Purpose Limitation: data collected and processed to be adequate and relevant for the purpose
5. Access and Correction: Individuals to have access to their personal information, and ability to seek correction of such personal information
6. Disclosure of Information: disclosure of personal information to third parties after providing notice and seeking informed consent
7. Security: reasonable safeguards to secure personal information
8. Openness: implement necessary steps in proportion to the scale, scope, and sensitivity of the data collected
9. Accountability: accountability for complying with security measures

1 https://pib.gov.in/newsite/PrintRelease.aspx?relid=88503
2 https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf
3 https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf

In 2017, through a unanimous judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[4], the Supreme Court of India recognized the right to privacy as an element of the fundamental right to life and personal liberty under Article 21, as well as stemming from the aspects of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III of the Indian constitution. However, the judgement also held that the right to privacy is not at an absolute right, and any incursion of privacy should meet three conditions viz., legality i.e., a legislative mandate, legitimate state aim, and proportionality. Meanwhile, the Ministry of Electronics and Information Technology (MeitY) constituted a Committee of Experts under the Chairmanship of Justice B N Srikrishna 'to study and identify key data protection issues and recommend methods for addressing them' and prepare a draft Data Protection Bill[5]. The committee submitted its report, titled 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' in 2018[6] along with the draft Personal Data Protection Bill, 2018[7].

The recommendations of the Srikrishna Committee Report along with suggestions from various stakeholders formed the basis of the Personal Data Protection Bill, 2019[8]. The Bill was introduced in parliament in December 2019 where it was referred to a Joint Parliamentary Committee (JPC) constituting of members from both houses of parliament for its suggestions. After several extensions and extensive consultations, the JPC released its report in 2021 wherein it undertook a clause-by-clause examination of the Bill to arrive at its final recommendations; and submitted a revised version of the Bill titled the Data Protection Bill, 2021[9]. The JPC proposed 81 amendments to the Bill and sought to expand the scope of the proposed law to include non-personal data, essentially altering the mandate from personal data protection to a broader form of data protection.

The Bill, as amended by the JPC was withdrawn from Parliament in August 2022 citing the significant amendments and recommendations of the JPC, along with concerns from Indian start-ups and the tech industry[10]. In November 2022, the Ministry of Electronics and Information Technology released the draft Digital Personal Data Protection Bill, 2022 for public consultation[11,12]. In August 2023, the Digital Personal Data Protection Bill, 2023 was introduced in Parliament. The Bill had a few key differences from the draft released for public consultation viz, personal data processing outside India would now be undertaken as per a country blocklist which would be notified by the Union Government, exemptions provided to the government for data processing activities were expanded, and the appeals process was reworked to designate the Telecom Disputes Settlement and Appellate Tribunal as the appellate tribunal to address appeals against decisions of the Data Protection Board constituted in the draft legislation. The Bill was passed by both houses, received the president's assent and became the Digital Personal Data Protection Act, 2023[13]. These landmark events are traced in Figure 1

4 https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

5 https://pib.gov.in/newsite/PrintRelease.aspx?relid=169420#:~:text=Recognising%20the%20importance%20of%20data,B%20N%20Srikrishna%2C%20Former%20Judge%2C%20Supreme

6 https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

7 https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

8 http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

9 https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

10 https://www.thehindu.com/sci-tech/technology/internet/explained-why-has-the-government-withdrawn-the-personal-data-protection-bill-2019/article65736155.ece

11 https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf

12 https://www.meity.gov.in/writereaddata/files/Notice%20-%20Public%20Consultation%20on%20DPDP%202022_1.pdf

13 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

Figure 1: Tracing Personal Data Protection in India

Source: IPCIDE staff

India's Data Protection Laws: A Controlled Comparative Analysis

Innumerable years and four iterations later, India's data protection law was finally enacted. The latest iteration that has become legislation, has changed considerably as compared to previous counterparts. Table 1 compares the four iterations of India's data protection law across 11 metrics in an attempt to demonstrate the diametrical changes and transition this law has undergone. This comparison is by no means meant to convey the nuance and complexity of each iteration, but serve to highlight the depth of change in the law over the years of legislative process, especially the sharp shifts in the Digital Personal Data Protection Act, 2023.

Table 1: A Comparative Analysis of the Various Iterations of Proposed Data Protection Laws in India: A Snapshot

Metric	Personal Data Protection Bill, 2018	Personal Data Protection (PDP) Bill, 2019	Data Protection Bill, 2021 - Recommendations of Joint Parliamentary Committee (JPC)	Digital Personal Data Protection Act, 2023
Scope	Includes processing of personal data within India; allows processing outside India, if it is for businesses offering goods and services, and activities involving profiling of data principals[14] in India.	Identical to the 2018 Bill, also includes certain anonymised personal data.	Over and above the scope of the 2019 Bill, includes processing of non-personal data and anonymised personal data.	Scope limited to processing of digital personal data within India where such data is collected online, or collected offline and is digitised. It will also apply to such processing outside India, if it is for offering goods or services in India. Does not apply to personal data that has been made publicly available by the individual to whom it relates.
Data breaches	Data Protection Authority (DPA) to be notified about a breach which is likely to cause harm; DPA will decide whether to notify the data principals or not.	Identical to the 2018 bill.	DPA to be notified about breaches, within 72 hours. DPA will decide whether to notify the data principals or not.	Data Protection Board of India (DPB) and data principals to be notified about breaches.
Right to be forgotten	Data principal will have the right to be forgotten.	Identical to the previous Bill	Identical to the previous Bill	Not provided.
Right to data portability	Data principal will have the right to data portability.	Identical to the previous Bill	Identical to the previous Bill	Not provided.
Data localisation	Classifies data into sensitive[15] and critical data[16]. One copy of personal data to be stored in India; Consent-based transfer outside India to certain permitted countries or under contracts approved by the Authority; Critical data can be processed only in India.	Allows cross-border transfer but a copy of sensitive personal data should remain in India; Critical personal data to be processed only in India; Certain sensitive personal data may be transferred if explicit consent is provided.	Allows cross-border transfer but a copy of sensitive personal data should remain in India; Critical personal data to be processed only in India; Sensitive personal data may not be transferred without prior approval of the central government.	Removes sensitive and critical personal data classification; The Central Government may restrict personal data flow to certain countries through notification.

14 Data principal means the individual to whom the personal data relates to

15 Sensitive data includes biometric, financial, health, affiliation, and orientation data. Also includes passwords.

16 To be defined by the government later.

Metric	Personal Data Protection Bill, 2018	Personal Data Protection (PDP) Bill, 2019	Data Protection Bill, 2021 - Recommendations of Joint Parliamentary Committee (JPC)	Digital Personal Data Protection Act, 2023
Exempted parties	Necessary, and proportionate exemptions for security of state (and legal proceedings, etc.) in accordance with the procedure established by law.	Builds on the 2018 Bill and allows the central government to exempt agencies where necessary, subject to certain procedure, safeguards and oversight.	In addition to the previous Bill adds reasonable and proportionate order that should specify a procedure, which is just and fair.	Expands exemptions in the interests of sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order, among other reasons. Allows the central government to exempt by notification; does not require any procedure or safeguards to be specified. Start-ups[17] can also be exempted by the central government.
Impact assessment	Provides for data protection impact assessment, that includes details and purpose of data processing, assessment of potential harm and measures for mitigating it.	Identical to the previous Bill	Identical to the previous Bill.	Not provided.
Institutions	Establishes Data Protection Authority of India (DPA) and an appellate body.	Identical to the previous Bill	Identical to the previous Bill	Establishes the Data Protection Board of India (DPB) and designates the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) as the Appellate Tribunal.
Harms	Defines harm that includes bodily and mental injury, monetary loss, identity theft, loss of reputation, loss of employment, any discrimination, and unreasonable surveillance; Data fiduciaries[18] to take measures to minimise and mitigate risks of harm.	Identical to the previous Bill	Identical to the previous Bill	Not provided.
Compensation	Data principal has a right to seek compensation in the event of harm.	Identical to the previous Bill	Identical to the previous Bill	Not provided; Modifies Section 43A (**compensation for failure to protect data)** of IT Act, 2000 and removes the provision of compensation.
Penalties	The Bill bifurcates penalties based on contravention of certain provisions; with up to INR 5 or 15 crore or 2% or 4% of worldwide turnover of the preceding financial year.	Identical to the previous Bill	Identical to the previous Bill	Financial penalties ranging from INR 50 crores to INR 250 crores depending on the nature of the breach.

Source: IPCIDE staff

17 Leaves to the central government to define start-ups.

18 Data Fiduciary means any person(s) who determines the purpose and means of processing of personal data.

Conclusion

The Digital Personal Data Protection Act, 2023 differs vastly from previous legislative efforts (Table 1). It has drawn criticism for an array of reasons such as narrowing the scope of the law to 'digital' personal data, concerns that massive exemptions have been granted to the Government that may have adverse implications for privacy, and several provisions in the Act being subject to determinations made by the Government.

The provisions of the Act are high-level and details around implementation will be laid out in the Rules. The Government should initiate a fair process of issuing Rules under delegated legislation by holding regular multi-stakeholder consultations.

OUR OFFICES:

4th Floor, Core 6A, India Habitat Centre, Lodhi Road,
New Delhi-110003
Plot No. 16-17, Pushp Vihar, Institutional Area, Sector 6,
New Delhi-110017

O: +91 11 43112400 / 24645218
F: +91 11 24620180 | **E:** ipcide@icrier.res.in
W: https://icrier.org/ipcide/