



Malavika Ramanand
Associate

DIGITAL PERSONAL DATA PROTECTION BILL, 2022 – AN ANALYSIS

PART II

A. Introduction

Part I¹ summarized the key features of Chapters I and II of the Digital Personal Data Protection Bill, 2022 (the **Bill**), which was issued by the Union Ministry of Electronics and Information Technology, on November 18, 2022. This *Connect* focuses on the remaining chapters.

B. Key Features

1. Obligations of a Data Fiduciary

Data Fiduciaries must:

- a. Comply with the provisions of the Bill when processing personal data;
- b. Make reasonable efforts to ensure accuracy and completeness of personal data being processed;
- c. Implement appropriate technical and organizational measures to prevent any breaches (The Bill is unclear on the standards of these measures);
- d. Notify the Data Protection Board (**DPB**) in the event of a personal data breach;
- e. Cease processing and retention of personal data, if purpose of processing is no longer served, and/or if retention is no longer necessary for the business;
- f. Publish contact details of the Data Protection Officer (**DPO**) in the manner prescribed;²
- g. Establish procedure to address grievances of Data Principals; and
- h. Engage third-party data processors only under valid contracts.

2. Significant Data Fiduciary and Related Obligations

The Bill introduces a new category of data fiduciaries called ‘significant data fiduciaries’ (**SDFs**), that will be notified by the Central Government (**CG**). SDFs will be classified based on the sensitivity and volume of data collected and processed, degree and risk of harm to Data Principals, impact on the sovereignty of India, *etc.* Additional obligations of SDFs are to:

- a. Appoint a DPO who will represent the SDF and be based in India;
- b. Appoint an Independent Data Auditor who will assess the SDFs’ compliance with the Bill; and
- c. Undertake ‘Data Protection Impact Assessments’³ and periodic audits, as may be prescribed.

3. Rights of Data Principal

The Bill provides rights to Data Principals as follows:

- a. **Right to Information:** Data Principals will have the right to obtain confirmation and a summary of personal data being processed by the Data Fiduciary, and processing actions undertaken. Data Principals may also request details of identities of all Data Fiduciaries with whom personal data was shared.

¹ *Counselence Connect*: Vol. 3, No. 38 of December 26, 2022.

² To be prescribed in the Rules.

³ This means an assessment which comprises of the description, purpose, assessment of harm, measures for managing risk of harm and other such matters with respect to processing of personal data.

- b. Right to Correction and Erasure: Data Principals can request their personal data to be corrected or erased. Upon receiving such requests, Data Fiduciaries must correct, complete, update and/or erase the personal data, accordingly.
- c. Right to Grievance Redressal: If a Data Principal is not satisfied with the response/handling of complaint by the Data Fiduciary, or if no response is received within seven days, they may register a complaint with the DPB, in the manner prescribed.
- d. Right to Nominate: A Data Principal may nominate an individual who can exercise their rights in the event of death or incapacity.

4. Duties of Data Principal

As a novel introduction, this Bill lists certain duties for Data Principles, which may be to impede any frivolous complaints. Accordingly, Data Principals must:

- a. Comply with the provisions of all applicable laws while exercising their rights;
- b. Not register false complaints;
- c. Not furnish false particulars or suppress material information while applying for documents, services *etc.*; and
- d. Only furnish verifiable information while exercising their right to correction or erasure.

5. International Transfer and Localization of Data

- a. The Bill permits international transfer of data to notified territories/countries. Personal data may be transferred in accordance with terms and conditions that are yet to be specified by the CG.
- b. In terms of localization, there is no requirement on part of Data Fiduciaries to process and store personal data only in India. This appears to be in contrast with the Personal Data Protection Bill, 2019, where there was a requirement for “critical personal data” to be processed and stored in India.⁴

6. Exemptions

The Bill exempts Data Fiduciaries from their notice and consent obligations for processing of personal data when: (i) it is necessary for enforcing legal rights or claims; (ii) it is necessary for the performance of any judicial or quasi-judicial function; (iii) it is processed pursuant to any contract entered into, with any person outside India, by a person based in India; and (iv) it is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of laws.

7. Compliance Framework

DPB:

- a. The DPB is characterized as the enforcement authority of the provisions of the Bill. The functions of the Board include (i) determining non-compliance and imposing appropriate penalties; (ii) performing functions determined by the CG; (iii) providing reasonable opportunity to Data Fiduciaries to be heard, and issuing directions; (iv) directing Data Fiduciaries to adopt urgent measures to remedy any breaches.
- b. The DPB must function as an “independent authority” and take actions against a Data Fiduciary or processor in accordance with the Bill.
- c. The directions of the DPB will be binding and shall be enforced as if it were a decree made by a Civil Court.⁵ Appeals against a DPB order shall be made to a High Court, and Civil Courts do not have jurisdiction to entertain suits under the Bill.
- d. If in the event a complaint may be better resolved by mediation or other processes of dispute resolution, then the DPB may direct parties to pursue the same.

⁴ Clause 33 of the Personal Data Protection Bill, 2019, accessible [here](#).

⁵ DPB shall have all powers of a Civil Court, as provided in the Code of Civil Procedure, 1908.

- e. The DPB may also accept a “voluntary undertaking” for a Data Fiduciary to undertake a particular action within a specified time, in relation to a compliance obligation. It is, however, unclear as to the circumstances under which an undertaking may be submitted.
- f. Since the DPB’s strength, composition, selection, conditions of service of its members, will be prescribed by the CG, the nature of its independence is questionable at this stage.

8. Penalties

- a. Financial penalties may be imposed by the DPB after factoring: (i) the nature, gravity, and duration of non-compliance; (ii) type and nature of the personal data affected by non-compliance; (iii) repeated nature of non-compliance; (iv) whether action to mitigate effects of non-compliance was taken by the Data Fiduciary.
- b. Schedule 1 to the Bill proposes financial penalties for non-compliance as below:

#	Subject of Non-Compliance	Penalty (INR)
1.	Failure of Data Fiduciary/Processor to take reasonable security safeguards to prevent breach	250 Cr. (\$300 Mn.)
2.	Failure to notify DPB and affected Data Principal(s) in the event of personal data breach	200 Cr. (\$240 Mn.)
3.	Non-Fulfilment of obligations of SDFs	150 Cr. (\$180 Mn.)
4.	Failure of Data Principals to adhere to their duties	10,000 (\$120 Mn.)
5.	Non-compliance with any other provision of the Bill and/or any rule made thereunder	50 Cr. (\$60 Mn.)

C. Conclusion

The Bill appears to be an accessible and ‘easy-to-read’ version compared to its former iterations. It seems to be a step forward in having comprehensive data protection framework in India, repealing sections 43A (*Compensation for failure to protect data*) and 87(ob) (*the reasonable security practices and procedures and sensitive personal data or information under section 43A*) of the Information Technology Act, 2000. Following public consultation, the CG may incorporate modifications to the Bill and introduce a revised version to the Parliament.

This Counsencence Connect contains information in a nutshell on a recent change in law. This is not legal advice and must not be treated so. For any clarifications, please contact us at: info@counsencence.com. Past issues of Counsencence Connect are available at the ‘Newsletters’ page of our website (www.counsencence.com).