

Summary – The Digital Personal Data Protection Act, 2023

On 3rd August 2023, the Digital Personal Data Protection (DPDP) Bill, 2023 was introduced in the Lok Sabha and passed on 9th August 2023, and subsequently introduced and passed on 9th August 2023 in the Rajya Sabha. On 11th August 2023, the President of India gave assent to the bill and henceforth known as the Digital Personal Data Protection (DPDP) Act, 2023.

The Act shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act.

This document is intended to provide a summary of the provisions of the Act along with a comparison with the DPDP 2022 Draft Bill of the same.

Chapter 1: Definitions and Scope

SUMMARY OF PROVISIONS: The DPDP Act 2023 will apply to the processing of digital personal data which is either collected in digitised form or collected in non-digital form and digitised subsequently. Foreign entities which process personal data to offer goods and services to Data Principals within the territory of India will also be subject to the DPDP Act 2023. However, the law does not apply to processing of personal data by an individual for any personal/domestic purposes, and to processing of publicly available personal data.

COMPARISON WITH 2022 DRAFT: In terms of extra-territorial applicability of the law, the Act applies to processing of digital personal data outside India where such processing takes place to offer goods or services to Data Principals in India. While the 2022 draft also governed any profiling of Data Principals in India, this has been omitted from the scope of the law. While the 2022 draft conflated the concept of Consent Manager and Data Fiduciary, the Act now clarifies that a Consent Manager refers to a *person* registered with the Board who acts as a single point of contact for the Data Principal for managing their consent.

Chapter 2: Obligations of Data Fiduciary

SUMMARY OF PROVISIONS: Data Fiduciaries are obliged to process personal data only for lawful purposes, either with the consent of the data principal or for certain legitimate uses. Data Fiduciaries must, either while or before seeking consent, provide data principals with a notice indicating the exact personal data being processed, along with the purpose for it. Consent Managers may be used by Data Principals for giving or reviewing consent and every Consent Manager is required to be registered with the Data Protection Board. There are some additional obligations imposed on Significant Data Fiduciaries such as the appointment of a Data Protection Officer based in India, and the responsibility to undertake measures such as Data Protection Impact Assessments.

COMPARISON WITH 2022 DRAFT: While the 2022 bill introduced the concept of ‘deemed consent’, the same has been revised under DPDP Act 2023 to indicate “certain legitimate uses” for which personal data can be processed. In addition to the parents of children, verifiable consent now must also be obtained by the Data Fiduciaries from the lawful guardians of persons with disabilities. The Central Government now also has the power to exempt a specific Data Fiduciary from any or all obligations relating to processing children’s data if the Data Fiduciary demonstrates that its data processing activities, pertaining to children, are verifiably safe.

Chapter 3: Rights and Duties of Data Principals

SUMMARY OF PROVISIONS: Data Principals have the right to access, seek correction and erasure of their personal data. Data Principals can also nominate another individual to exercise their rights on their behalf in the event of their death or incapacity. Data Principals are also entitled to a grievance redressal mechanism to address grievances against Data Fiduciaries and Consent Managers. Duties of Data Principals include ensuring compliance with applicable laws while exercising rights, refraining from impersonating other individuals, and not suppressing material information from the State or its instrumentalities. Additionally, the Data Principals are obliged to not misuse redressal mechanisms by lodging false or frivolous complaints and to furnish only verifiably authentic information when seeking to correct or erase their personal data.

COMPARISON WITH 2022 DRAFT: The 2023 Act highlights that the Data Principal’s right to access information is not absolute. Data fiduciaries may, under authorisation of any law, share personal data with other data fiduciaries for the purpose of prevention, detection, or investigation of offences and cyber incidents. The right of a data principal to access information does not extend to any data processing and data sharing which has been undertaken for the above purposes. The current Act envisages the provision of grievance redressal mechanisms by Consent Managers in addition to Data Fiduciaries. While DPDP bill 2022 obliged the Data Fiduciaries to respond to grievances received within seven days, the current Act does not provide any defined time limit.

Chapter 4: Special provisions

SUMMARY OF PROVISIONS: On data transfers, it is stated that the Central Government, by notification, may restrict the transfer of personal data to certain jurisdictions. If there are higher degrees of protection warranted under other laws, then such other laws will prevail over the DPDP Act 2023.

The processing of personal data for certain purposes has been exempted from being subject to certain provisions of the Act. These exemptions include processing of personal data for enforcing a legal right, for the purposes of prevention, detection, investigation or prosecution of any offence, processing necessary for approved merger of companies, etc. There is specific mention of the power of the Central Government to exempt startups from being obligated to comply with some of the provisions of the law.

COMPARISON WITH 2022 DRAFT: The safe listing approach for data transfers has been reconsidered. In its place, the notion of a negative list is proposed, i.e., a list of countries to which personal data cannot be transferred. Two key changes to exemptions include the specific mention of startups as possibly being

exempt from some obligations, as well as the broader power of the Central Government to, through notification, exempt any Data Fiduciary from being subject to any provision of the law for a specified period.

Chapters 5-8: Compliance and Adjudicatory Framework

SUMMARY OF PROVISIONS: The operational and functional contours of the Data Protection Board have been outlined, including provisions around salaries, disqualifications, and resignations of members of the Data Protection Board. The powers and functions of the Board include receiving complaints regarding personal data breaches, inquiring into breaches of obligations under the law, and imposition of penalties for the same.

COMPARISON WITH 2022 DRAFT: The provisions of the DPDP Act 2023 provide greater clarity on the expertise of the Members to be appointed to the Data Protection Board. In contrast to the 2022 version, where appeals against decisions of the Board lied with the High Court, the 2023 Act prescribes that the Telecom Disputes Settlement and Appellate Tribunal shall act as the appellate body for data protection issues.

Chapter 9: Miscellaneous

SUMMARY OF PROVISIONS: This Chapter includes provisions on protecting the Central Government, the Board, its Chairperson and any Member, officer or employee against legal proceedings for actions taken in good faith, permitting the Central Government to call for information from any Data Fiduciary, creating a mechanism for blocking access to computer resources in case of repeated instances of non-compliance, and enabling the Central Government to notify rules on a number of issues.

COMPARISON WITH 2022 DRAFT: When contrasted against the 2022 draft, this Act introduces certain new provisions which create certain additional powers for the Central Government. There are two key additions here; *first*, the power of the Central Government to require any Data Fiduciary to furnish such information as may be called for and *second*, the power of the Central Government to block access to any information in any computer resource that enables a Data Fiduciary to offer goods or services to Data Principals within India. The latter power can be exercised against a Data Fiduciary, on written reference from the Data Protection Board, if monetary penalties have been imposed against the Data Fiduciary in two or more instances.
