Key Highlights of the Digital Personal Data Protection Act, 2023[1]

Introduction

The Digital Personal Data Protection Act (the "**Act**"), was passed in the Indian Parliament and notified by the Central Government on August 11, 2023. It draws extensively from the Digital Personal Data Protection Act, 2022, and is centred around safeguarding digital personal data. This Act comprising of 44 sections and 9 chapters is set to replace Section 43A of the Information Technology Act, 2000, as well as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data of Information) Rules, 2011 (SPDI Rules).

The Act applies to processing of digital personal data within India, as well as to the processing of digital personal data outside India if it is in connection with any activity related to the offering of goods or services to Data Principals (data subjects) in India. In this reference, the Act acknowledges and permits cross-border transfer of personal data by a Data Fiduciary to any country or territory for processing except if the Central Government restricts such transfer to any notified countries. This is similar to the General Data Protection Regulation (GDPR) of the European Union, which also allows cross-border transfer of personal data, but only to countries that have been deemed to have adequate data protection laws.

The Act is based on the following foundational principles:

1. **Purpose limitation**: Personal data should only be processed for a lawful purpose for which the Data Principal has given her consent and the purpose is in accordance with the Act and

2. **Collection limitation**: Only such personal data should be collected which is necessary. The limit and nature of personal data collected must not be more than what is required for the specified purpose.

3. **Apprised Consent**: Personal Data can only be processed after apprised and active consent is sought from the Data Principal. However, the Act also provides for Deemed Consent in certain named purposes and situations.

Applicability of the Act

The Act does not apply to personal data processed by an individual for any personal or domestic purpose, or personal data made publicly available by the Data Principal herself or any other person under a legal obligation and further does not make a distinction between different categories of personal data, such as sensitive personal data or critical personal data.

Consent as an Integral Element

Consent is the underlying basis for processing personal data under the terms of the Act and is required to be *free, specific, informed, unconditional and unambiguous*. The Data Principal has the right to withdraw consent at any time with the same level of ease with which she gave her consent. The Act mandates seeking of such consents through an active notice to the Data Principal informing the Data

[1] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)

Principal about the proposed purpose of the processing, the manner in which she may exercise her rights to withdraw consent and avail the grievance redressal mechanism or to make a complaint to the Data Protection Board.

Exception to Apprised Consent - Legitimate Uses and Deemed Consent

For certain "**Legitimate Uses**", a Data Fiduciary can be exempted from obtaining prior consent from a Data Principal. Such legitimate uses include processing for purposes of employment, responding to medical emergencies, performing any function under law or the State providing any service or benefit to the Data Principal, and compliance with any judgment or order issued under any law, among others.

The Act allows for "**Deemed Consent**" in certain cases, such as when the data is collected for the purpose of providing a service or benefit to the Data Principal. This means that the Data Principal's consent is not required for the processing of their personal data in these cases.

Notifying Class of Data Fiduciaries as Significant Data Fiduciaries – Additional Obligations

The Act further empowers the Central Government to notify any or a class of Data Fiduciaries as significant Data Fiduciaries based on multiple metrics (such as volume and sensitivity of personal data processed, risk to the rights of the Data Principal, security of state, etc.). Such notified Significant Data Fiduciaries need to comply with additional requirements such as – appointing an individual as a Data Protection Officer based in India, appointing an independent data auditor to evaluate compliance with the Act, conducting periodic audit and data protection impact assessments, and undertaking other measures including periodic data protection impact assessments.

Obligations of Data Fiduciaries

Data Fiduciaries are required to conduct all their activities within the bounds of the act. They are further also required to delete personal data in case the Data Principal withdraws her consent or if it is reasonable to assume that the specified purpose is no longer being served unless such retention is necessary for compliance with any law. In case of any breach in personal data, they are required to inform the Data Protection Board and each affected Data Principal of such breach and offer readily available grievance redressal mechanisms to affected Data Principals.

Permitting Agency Representation for both Data Principals and Data Fiduciary

The Act allows Data Fiduciaries as well as Data Principals to appoint agents in the form of Data Processors and Consent Managers respectively, to manage their set of obligations under the Act efficiently.

Rights of Data Principals

Data Principals being the main stakeholders, have been provided with various rights to safeguard and protect the processing of their personal information. Such rights include the right to access information about personal data including a summary of personal data being processed, the underlying processing activities and any other information as prescribed, and identities of all Data Fiduciaries and Data Principals with whom such data was shared; the right to correction and erasure

of personal data; right to nominate an individual to exercise rights on their behalf in the event of their death or incapacitation.

Data Processing of Children

To protect the presence of minors and people with disabilities on online platforms, the Act mandates seeking verifiable consent of parents/ lawful guardians to process personal data of children and persons with disabilities. To further protect the interest of their impressionable mind, the Act prohibits the tracking or behavioural monitoring of and targeted advertising directed at, children, and processing of children's data that is likely to cause any detrimental effect on the well-being of a child.

Cross-Border Transfer

As has been pointed out, the Act allows Data Fiduciaries to transfer data to any other country for processing personal data unless such a country is not restricted (blacklisted) by the central government.

General Powers of Central Government

The Act gives the Central Government very wide powers to regulate the processing of personal data. The government can, for example, restrict the cross-border transfer of personal data, require data fiduciaries to take certain security measures call for any information from the Data Protection Board, the Data Fiduciary or any intermediary, and even direct data fiduciaries to delete personal data. In public interest, the Central Government can even block public access to information on a platform.

Grievance Redressal Mechanism

The Act contemplates the establishment of a Data Protection Board ("**DPB**"), as an enforcement and dispute redressal body which will have powers, inter alia, to direct any urgent remedial or mitigation measures on receipt of intimation regarding a personal data breach, inquire into such breach, impose penalties for non-compliance, advisory and make recommendation for blocking public access if a Data Fiduciary has been fined more than twice, inspect any document, summon and enforce the attendance of any person etc. Individuals aggrieved under the law will be required to first approach the grievance redressal mechanism provided by the Data Fiduciary. After exhausting this option, they will be allowed to approach the Board.

The Act has also provided for appeals, which will lie before the Telecom Disputes Settlement and Appellate Tribunal.

Penalties for Non-Compliance

The Board has been empowered to impose monetary penalties of up to **INR 250 crores** for non-compliance with the Act. The penalties will be credited to the Consolidated Fund of, which means that individuals who have been harmed by data breaches or other violations of their data privacy rights will not be compensated, instead defaulting Data Fiduciaries will be liable to pay penalties for their default, which will be credited to the Consolidated Fund of India.

The scope of compensation as relief has been done away with, and Section 43A of the Information Technology Act, 2000, which provided for compensation has been explicitly repealed.

Conclusion

In summary, the Act represents a significant step forward in addressing the complexities of data protection in the digital age. It aims to strike a delicate balance between individual privacy and the legitimate needs of businesses and government agencies. As India adapts to this new regulatory landscape, it will be crucial to monitor its implementation and any potential challenges that may arise, and to ensure that the Act achieves its intended objectives of safeguarding personal data while fostering innovation and economic growth in the country.