
The Digital Personal Data Protection Bill: Embarking towards a new Framework

Bhawna Singh
LLM (Corporate, Financial Law & Policy)

Introduction

‘Data’ a term which is a combined result of statistics or information collated for reference on any particular subject matter. Everything today is revolving around data, has given access of data to industries for commercial requirements. The need for data centre is increasing quickly as India accelerates its transition to a digital economy. Given the surge in cloud use and data consumption, businesses are aggressively investing in these assets. Their readiness to build data centre for data storage and deployment has created a favorable environment for India to become a global hub.

With this new accelerated usage of data, it requires stringent rules for the protection of the same. Since 2018, the Indian government has been working on enacting a comprehensive data protection law. Prior to the present text of the current data bill, three drafts were released. The 2022 Bill, like the 2021 Bill, allows for the processing of digital personal data in a way that recognizes individuals' right to personal data protection, social rights, and the necessity to handle personal data for authorized purposes.¹ The current bill differs significantly from previous iterations in that it is more leaving majority of granular aspects to set out by way of subsequent rule making. The 2022 Bill pertains to the processing of digital personal data on Indian territory, whether obtained online or offline from data principal and then digitized. The 2022 Bill does not apply to personal data gathered offline; it solely controls the processing of personal data obtained online or in digital form.² The DPDP Law establishes an independent Board, known as the Data Protection Board, to serve as an adjudicating authority to enforce the Bill's requirements and levy penalties in situations of noncompliance.³ In the case of a breach of personal data, the Board has been granted the authority to require the data fiduciary to take whatever immediate action to remediate the breach or minimize any harm caused to data principals.

Guidelines of The Digital Personal Data Protection Bill, 2022

The proposed law is intended to have extraterritorial applicability, which means that it applies to the processing of personal data outside India where such processing is in conjunction with

¹ Rachit, Rohan and Archana, “Comparing The Digital Personal Data Protection Bill, 2022 With The Data Protection Bill, 2021” Mondaq, available at <https://www.mondaq.com/india/data-protection/1269900/comparing-the-digital-personal-data-protection-bill-2022-with-the-data-protection-bill-2021>

² Ibid

³ Seema Jhingan and Jyoti Vats Mishra, “A Dive Into The Digital Personal Data Protection Bill, 2022” Mondaq available at <https://www.mondaq.com/india/data-protection/1259392/a-dive-into-the-digital-personal-data-protection-bill-2022>

any profiling of, or offering products or services to data principals residing inside India's territory.⁴ Personal data can only be transmitted to countries that have been registered by the Central Government, and only under certain conditions.⁵ Having said that, this will come as a big relief for companies who need to send out data's across borders. There is a possibility of cross-border data migration outside India in a globalized economy where data collecting has become an integral part of daily transactions. The 2022 Bill makes no mention of a comprehensive legal framework for the cross-border transfer of digital personal data.⁶ The proposed bill would be the latest regulation that might affect how tech conglomerates like Facebook and Google process and transfer data in India's rapidly expanding digital economy.⁷ While the removal of data localization requirements under the 2022 Bill is a welcome step towards allowing the free flow of data, it is unclear whether the proposed legislation will allow cross-border transfers to countries that have not been whitelisted by the government.⁸

The European Data Protection Guidelines

Having regard to the General Data Protection Regulation Article determines the geographical scope of the Regulation, which constitutes a fundamental evolution of EU data protection legislation.⁹ The EDPB guidelines establish the parameters for assessing the applicability of the GDPR's territorial scope. A uniform interpretation is also required for controllers and processors, both within and outside the EU, in order to determine whether they must comply with the GDPR for a certain processing activity.¹⁰ The EDPB maintains, as a general principle, that if personal data processing comes within the geographical area of the GDPR, all requirements of the Regulation apply to such processing.¹¹ In the case of a data processor established in the Union processing on behalf of a data controller established outside the Union and not subject to the GDPR as per Article 3(2), the EDPB considers that the data controller's processing activities would not be deemed to fall within the territorial scope of the GDPR simply because it is processed on its behalf by a processor established in the Union.¹² While the current guidelines attempt to explain the GDPR's territorial scope, the EDPB wishes to emphasize that controllers and processors must also consider other applicable documents, such as EU or Member States' sectorial legislation and state laws.¹³

⁴ Section 4(2) of The Digital Personal Data Protection Bill, 2022

⁵ Section 17 of The Digital Personal Data Protection Bill, 2022

⁶ The Digital Personal Data Protection Bill, 2022

⁷ Reuters, "India proposes easier cross-border data transfers under new privacy law" <Business Standard> 18th November 2022

⁸ Rachit,Rohan and Archana, "Comparing The Digital Personal Data Protection Bill, 2022 With The Data Protection Bill, 2021" Mondaq, available at <https://www.mondaq.com/india/data-protection/1269900/comparing-the-digital-personal-data-protection-bill-2022-with-the-data-protection-bill-2021>

⁹ The European Data Protection Guidelines

¹⁰ Ibid

¹¹ Ibid

¹² Ibid

¹³ Ibid

On the outset, the Board in case discovers major non-compliance by a person after conducting an inquiry, it may impose a pecuniary penalty of up to INR 500 crore.¹⁴ The proposed law also imposes specific penalties ranging from INR 50 crore to INR 250 crore for failing to implement reasonable security safeguards to prevent personal data breaches, failing to notify the Board and affected data principals of data breaches, and failing to comply with additional obligations for SDFs.¹⁵ The most severe penalties under the Proposed Law are for failing to comply with the Proposed Law's data-breach responsibilities.

Conclusion

The Digital Personal Data Protection Bill is an attempt by the Government to establish a clearly stated and intelligible law on data protection in the country as compared to the preceding PDP Law which was attacked by enterprises and start-ups for being compliance intensive. When processing personal data in the interests of India's sovereignty and integrity, security of the state, friendly relations with other states, preservation of public order, or avoiding incitement to any cognizable offence pertaining to any of these, a complete exemption can be allowed.¹⁶ Nevertheless, in an effort to reduce the size of the prior draft, the DPDP Law failed to elaborate the key clauses.

¹⁴ Section 9(5) of The Digital Personal Data Protection Bill, 2022

¹⁵ Section 25(1) of The Digital Personal Data Protection Bill, 2022

¹⁶ Trishee Goyal, "How different is the new data protection Bill?", The Hindu; available at <https://www.thehindu.com/sci-tech/technology/how-different-is-the-new-data-protection-bill/article66166438.ece>