DATA PROTECTION LAWS IN INDIA AND ITS IMPACT ON EMPLOYEES AND EMPLOYERS

Vivek Prem Daswaney[1], Dr. Harita Shinde Bangali[2]

[1]*Ph. D. Research Scholar*
School of Law, Sandip University, Nashik, Maharashtra, India.
[2]*Associate Professor, Research Guide*
School of Law, Sandip University, Nashik, Maharashtra, India.

ABSTRACT

By way of bringing forth the new data protection laws in India, the country marks a noteworthy milestone in the growth of data protection laws. This paper examines the impact of India's Digital Personal Data Protection Act, 2023[1] ("DPDP Act") and the draft Digital Personal Data Protection Rules, 2025[2] ("DPDP Rules") on the employer-employee relationship.

The article provides an overview of the DPDP Act and DPDP Rules and highlights notable provisions related to notice, data principal rights, significant data fiduciaries, contact information, and data erasure. It also analyzes the impact of these regulations on both, Employees, who gain control, transparency, and protection of their data and Employers, who face compliance burdens, the need for data processing policies and greater accountability.

INTRODUCTION

The rapid expansion of digital India has profoundly impacted the lives of Indian citizens and transformed the lives of Indian citizens and governance in general. Digital India has not only fostered innovation and entrepreneurship within the digital realm but also attracted the significant presence of large global big tech platforms.

Data and Personal Data in specific are at the core of this fast-growing digital economy and eco-system of digital products, services and intermediation. It has become very clear over the last few years that data and Personal Data must be subject to a framework of rules with the dos and don'ts.

The increasing reliance on technology has made data protection a critical issue for organizations worldwide. In response to the growing concerns about data security, privacy breaches, and the ethical use of personal information, the DPDP Act and DPDP Rules were introduced.

[1] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), *Gazette of India*, August 11, 2023.
[2] The Digital Personal Data Protection Rules, 2025 (India).

The DPDP Act and the DPDP Rules are aimed to establish a balance between the needs of the employers and the fundamental rights of the employees regarding data privacy while ensuring robust data protection standards. The DPDP Act provides the foundational legal framework for data privacy in India whereas the DPDP Rules outline the specific procedures and implementation guidelines for operationalizing the DPDP Act.

This paper will aim to primarily highlight the overview of the DPDP Act and the DPDP Rules and its impact on both employees and employers and the transformations the DPDP Act and the DPDP Rules have made to manage and protect personal data.

BRIEF OVERVIEW ON THE DATA PROTECTION ACT

The DPDP Act applies to digital and digitised forms of Personal Data that is within the territory of India. The DPDP Act defines 'Personal Data' as any data about an individual who is identifiable by or in relation to such data. This would mean someone's physical identifiers, email address, phone number, Aadhar/ PAN no., residential address, IP address, etc.

Therefore, any organization that processes Personal Data of an individual who is within the territory of India must comply with the provisions of the DPDP Act. The DPDP Act also has extra-territorial jurisdiction similar to the GDPR as it shall also apply to processing of Personal Data that is outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to individuals within the territory of India.

KEY TERMS UNDER THE DPDP ACT:

1. Who is a Data Principal?
   This refers to an individual to whom the Personal Data relates to or belongs to.

   The DPDP Act clarifies that where this Personal Data belongs to a child or a person with a disability, the Data Principal shall be the lawful guardian.

2. Who is a Data Fiduciary?
   This refers to the person / organization who alone or in conjunction with other persons/ companies determines the purpose and means of processing of Personal Data.

   The DPDP Act also specifies that the Central Government may by a notification classify some Data Fiduciaries as Significant Data Fiduciaries on factors such as the volume and sensitivity of Personal Data processed by them, the risk to the rights of a Data Principal, risk to public order etc. The Central Government will impose such additional obligations on the Significant Data Fiduciary as it may deem necessary for compliance of the provisions under the DPDP Act.

3. Who is a Data Processor:
   It refers to any person / organization who processes Personal Data on behalf of a Data Fiduciary.

4. Who is a Consent Manager:
   It refers to a person registered with the Data Protection Board of India. Its primary function is to act as a single point of contact to enable a Data Principal to give, manage, review and withdraw their consent through an accessible, transparent and interoperable platform.

5. What is Processing:
   It refers to any action done to Personal Data. In a broader sense it could cover just about anything you can do with data: collection, storage, transmission, analysis, organization, indexing, sharing, etc.

BRIEF OVERVIEW ON THE DATA PROTECTION RULES

The DPDP Rules are a set of regulations that operationalize the DPDP Act in India. It provides a detailed framework for implementing the principles and provisions outlined in the Act.

NOTABLE PROVISIONS OF THE DPDP RULES:

1. **Notice given by the Data Fiduciary to Data Principal:** The DPDP Rules place significant emphasis on obtaining valid consent from the Data Principal before processing their personal data. The notice provided by the Data Fiduciary to the Data Principal must be understandable and distinct from any other information shared by the Data Fiduciary. It must be in clear and plain language so as to provide the Data Principal with a full and transparent account of the information necessary for giving their informed consent for the processing of their personal data. The notice should also include, an itemized description of the personal data being collected and clear description of the purpose for processing, along with an itemized explanation of the goods or services or uses enabled by such processing.

2. **Rights of Data Principals:** The Data Fiduciary and the Consent Manager shall clearly publish on their website or app the process by which the Data Principals can exercise their rights under the DPDP Act. Data Principals can request to access and erase their personal data by contacting the Data Fiduciary. The Data Fiduciary must also provide clear timelines for responding to the grievances, ensuring an effective process with the necessary technical and organizational safeguards. Data Principals may also nominate one or more individuals to exercise their rights under the law, by complying with the procedures set by the Data Fiduciary and such other relevant laws as may be applicable.

3. **Additional obligations of Significant Data Fiduciaries:** This provision imposes specific responsibilities on the Significant Data Fiduciaries. It mandates that these Fiduciaries must conduct a Data Protection Impact Assessment (DPIA) and a comprehensive audit once every year. The findings of these assessments and audits, detailing their adherence to data protection requirements, must be reported to the Data Protection Board of India (DPBI). Further, the Significant Data Fiduciaries are held accountable for verifying that any algorithmic software they use for processing personal data does not pose a risk to the rights of Data Principals. This includes algorithms used for data hosting, storage, and sharing. Such Entities must adopt measures to ensure that personal data identified by the Central Government is processed in compliance with specific restrictions, ensuring that the data and any related data are not transferred outside of India.

4. **Contact information for addressing data processing queries:** Every Data Fiduciary must clearly display on their website or app the contact details of a designated person who can address questions regarding the processing of personal data. This could be the Data Protection Officer (DPO), if applicable. The contact information should be easily accessible and visible to Data Principals and the same contact details must be included in all responses to communications from Data Principals who wish to exercise their rights under the DPDP Act. The intent of this provision is to ensure transparency and accountability in data processing practices of Data Fiduciaries.

5. **Time period for specified purpose to be deemed as no longer being served:** Under this provision, personal data must be erased if a Data Principal does not engage with the Data Fiduciary within a specified period, unless required for legal compliance. Entities like e-commerce platforms, gaming intermediaries, and social media may retain data for up to three years from the last interaction or the coming in effect of rules, whichever is later, unless when the data is needed for the principal too access their account. Data Fiduciaries must notify the Data Principal 48 hours before erasure, providing an opportunity to preserve their data.

IMPACT OF THE DPDP ACT AND THE DPDP RULES ON THE EMPLOYEES AND EMPLOYERS

EMPLOYEES:

1. **Framework of Rights:** Employees now have a defined set of rights over their personal data, which employers are legally obligated to guarantee. These rights include the ability to demand completeness, accuracy, and consistency of their data, particularly when that data is used in decision-making processes that affect them or when their data is shared with another data fiduciary.

2. **Control over Personal Data:** Employees gain significant control over their personal data held by employers. They can exercise rights to access, correct inaccuracies, and request erasure of their data (with certain limitations, such as when data is needed for legal obligations or ongoing investigations).

3. **Transparency and Notice:** Employers are legally obligated to provide clear and accessible notices detailing their practices for collecting, using, and processing employee data. This enhanced transparency empowers employees to understand the full extent of data processing activities and make informed decisions regarding their personal information.

4. **Protection of Sensitive Personal Data:** The DPDP Act and the DPDP Rules establish stronger safeguards for protection of sensitive personal data like biometric information, health records, and financial details. This ensures that such data is handled with greater care and only processed when absolutely necessary for legitimate purposes.

5. **Grievance Redressal Mechanism:** Employees have the right to formally raise grievances with their employers regarding data privacy concerns. If they remain unresolved, they can escalate

these concerns to the Data Protection Board of India (DPBI), providing a formal channel for addressing data protection violations.

EMPLOYERS:

1. **Increased Compliance Burden:** Employers face a greater compliance burden to adhere to the DPDP Act and DPDP Rules. This includes implementing robust data protection measures, obtaining valid consent wherever required, ensuring data accuracy, implementing security safeguards, and establishing grievance redressal mechanisms.

2. **Need for Clear Data Processing Policies:** Employers must implement comprehensive data processing policies that are clear, transparent, easily accessible to employees, and compliant with the regulations. These policies should cover all aspects of employee data handling, from collection to its erasure.

3. **Increased Accountability and Potential Penalties:** Employers are held accountable for data privacy violations and face potential penalties for non-compliance. This emphasizes the importance of prioritizing data protection and implementing effective compliance measures.

4. **Need for Employee Training and Awareness:** Employers must invest in training their staff on data protection practices and the specific requirements of the DPDP Act and Rules. This ensures that all employees understand their roles and responsibilities in maintaining data privacy.

5. **Managing Employee Data Requests:** Employers need to establish efficient and timely procedures for handling employee requests related to their data, such as access, correction, and erasure requests. This requires having systems in place to locate, retrieve, and process data accurately and within the stipulated timeframes.

6. **Managing Consent and Legitimate Use:** Employers need to carefully consider the legal basis for processing employee data. While consent is one option, the Act also allows for processing data for certain “legitimate uses” related to employment. Employers must clearly define and document these legitimate uses to justify processing without explicit consent in certain situations.

It is quite clear from the DPDP Act and the DPDP Rules that any processing of personal data is the primary responsibility of the Data Fiduciary. This means that Employers bear the responsibility for the data processing activities of their Data Processors. It is therefore crucial for organizations to examine both their internal handling procedures and their external data flows.

CONCLUSION

The DPDP Act and DPDP Rules mark a transformative era in the regulation of personal data management for employers and employees alike. These legal frameworks promote responsible data handling practices and ensure greater transparency. Employers must navigate complex regulatory landscapes while employees gain increased protection and control over their personal data. Organizations that prioritize adherence to these regulations not only achieve legal compliance

but also build stronger relationships based on trust and accountability. In an increasingly data-driven world, fostering a balanced approach to data protection is essential for growth and a sustainable workplace environment.

The DPDP Act and DPDP Rules, once enacted shall impose stricter requirements on how personal data is processed, stored and transferred. Under this new act and rules, entities that process personal data will be required to adhere to heightened security practices and data subject rights. By mandating stricter compliance measures and guidelines, penalties and higher fines can be imposed for violation of data protection norms for any non-compliance.

REFERENCES

1. Briefing, I. (2024, July 15). *India's Digital Personal Data Protection (DPDP) Act, 2023*. India Briefing News. https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/

2. Burman, Anirudh. Understanding India's new data protection law. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en

3. Digital Personal Data Protection Act 2023 Compliance Checklist. (2025, January 10). RSM India. https://www.rsm.global/india/insights/consulting-insights/digital-personal-data-protection-act-2023-compliance-checklist

4. Digital Data Protection. (n.d.). https://innovateindia.mygov.in/digital-data-protection/

5. Draft Digital Personal Data Protection Rules. (n.d.). https://pib.gov.in/PressReleasePage.aspx?PRID=2090271

6. Unknown. (2025). Explanatory note to Digital Personal Data Protection Rules, 2025. https://www.meity.gov.in/writereaddata/files/Explanatory-Note-DPDP-Rules-2025.pdf

7. Indulia, B. (2024, November 11). Digital Personal Data Protection Act, 2023: A ready reckoner for employers | SCC Times. SCC Times. https://www.scconline.com/blog/post/2024/11/11/digital-personal-data-protection-act-2023-employers-guide/#:~:text=The%20DPDP%20Act%20applies%20to,information%2C%20identity%20proof%2C%20etc.

8. L. &. W. (2024, January 29). India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison | Global Privacy & Security Compliance Law Blog. Global Privacy & Security Compliance Law Blog. https://www.globalprivacyblog.com/2023/12/indias-digital-personal-data-protection-act-2023-vs-the-gdpr-a-comparison/

9. Manikanta, K. (2017). *Digital India Programme and Impact of Digitalization in Improving Quality of Life of Citizens.* Adarsh Journal of Management Research.

10. Pradeep, R. (2024, May 28). *Handle with CARE: Relying on "Purposes of Employment" for Processing Employee Data | India Corporate Law*. India Corporate Law.

11. Rao, K. S. (2023, August 21). Digital Personal Data Protection Act 2023 – A game changer. Times of India Blog. https://timesofindia.indiatimes.com/blogs/kembai-speaks/digital-personal-data-protection-act-2023-a-game-changer/

12. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Official Journal of the European Union, May 4, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

13. Solanki, S., & Solanki, S. (2024, June 25). *India's Data Protection in the Workplace and its Impact on Employers - Deepstrat*. Deepstrat. https://deepstrat.in/2024/06/25/indias-data-protection-in-the-workplace-and-its-impact-on-employers/

14. Sharma, J. (2016*). Digital India and Its Impact on Society.* Research in Humanities & Social Sciences.

15. The Digital Personal Data Protection Bill, 2023. PRS Legislative Research. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

****