THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: KEY IMPLICATIONS FOR EMPLOYERS

1. INTRODUCTION

a. After several years of deliberation, the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") received the President of India's assent on August 11, 2023, although its effective date is yet to be notified. Currently, the Government is in the process of framing the major rules under the DPDP Act, which are likely to be published soon.[1] Once the relevant sections are brought into force, the DPDP Act will repeal the Information Technology (*Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)* Rules, 2011 enacted under the Information Technology Act, 2000, which is the prevailing legislation in India governing the processing of personal data and sensitive personal data.

b. The DPDP Act has been enacted with the intent to hold businesses and organisations accountable and responsible for protecting the personal data of individuals that are collected by them during the course of their operations (*whether externally or internally*). This landmark development in India's data protection regime, once implemented, will bring India at par with other jurisdictions such as Singapore, People's Republic of China, the UK, and 27 of the EU Member nations, which have already enacted robust data protection laws.

2. EMPLOYER OBLIGATIONS UNDER THE DPDP ACT

a. APPLICABLE PROVISIONS OF THE DPDP ACT

(i) The DPDP Act defines 'personal data'[2] as any data about an individual who is identifiable by or in relation to such data and applies to the processing of all personal data within India when collected from data principals in digital form or in non-digital form and subsequently digitized. The DPDP Act is also applicable to the processing of digital personal data outside India if it relates to the offering of goods or services to data principals located in India. The DPDP Act does not apply to personal data that is made publicly available by a data principal. [3]

(ii) An employer collects a significant amount of personal data from its employees as well as potential employees during the lifecycle of employment, such as personal data collected during the employment application and interview process, during the onboarding formalities, for conducting background verification, for processing payroll, undertaking statutory compliances, and even during the time of the end of employment. Often,

[1] The Minister of State for Electronics and Information Technology has recently announced that the rules corresponding to the DPDP Act are anticipated to be notified by the end of January 2024. More information on this can be accessed here.
[2] Section 2(t) of the DPDP Act.
[3] Section 3 of the DPDP Act.

employers outsource several processes to third parties like background verification or compliance formalities or payroll operations that results in disclosure of personal data of their present or potential employees.

(iii) Under the DPDP Act, an employer processing any personal data of its employees would be considered as a 'data fiduciary' as they determine the purpose and the means of processing the data.[4] The employees in turn would be considered 'data principals' as they are the individuals to whom the personal data relates. Where an employer engages a third party to process the personal data of employees on their behalf, such a third party would be a data processor[5] under the DPDP Act.

b. **GROUNDS FOR PROCESSING PERSONAL DATA**

(i) ***Grounds for Processing***: Under the DPDP Act, an employer (*in the capacity of a data fiduciary*) may process the personal data of its employees for a lawful purpose under the following circumstances: (1) where they have voluntarily given their consent[6] to the processing of data; or (2) for certain legitimate uses provided under the DPDP Act.[7] Under the DPDP Act where consent is required for personal data, the processing of personal data has to be preceded by a specific request for consent along with a notice to the data principal setting out prescribed particulars involving the processing activities being undertaken.

(ii) ***Legitimate* Uses**: The DPDP Act also provides for certain grounds for processing personal data, where consent is not mandatorily required, categorized as 'legitimate uses' under the DPDP Act. Some of the prescribed legitimate uses that are relevant for employers have been summarized below:

1. Prevention of corporate espionage.
2. Maintenance of confidentiality of trade secrets, intellectual property, and classified information.
3. Provision of any service or benefit sought by a data principal (*employee*, *consultant*, *vendor*).
4. Complying with any judgment, decree, or order issued under any Indian law, and any judgment, decree, or order relating to claims of a contractual or civil nature under any law in force outside India as well.
5. Purposes of 'employment'.
6. Specified purposes for which the data principal has voluntarily provided their personal data to the data fiduciary (*i.e., the employers in this case*), and in respect of which they have not indicated to the data fiduciary that they do not consent to the use of their personal data.

c. **EMPLOYMENT PURPOSES AS A LEGITIMATE USE:**

(i) For processing personal data for "the purposes of employment", an organization is not required to obtain the consent of its employees (*data principal*). The DPDP Act does not provide any specific list of "purposes of employment" for which personal data can be processed without consent.

(ii) In the absence of such a requirement and unless further clarifications are provided under the rules, it seems that organizations have been provided with a blanket exemption to process the personal data of their

[4] Section 2(i) of the DPDP Act.
[5] Section 2(k) of the DPDP Act.
[6] As per Section 6(1) of the DPDP Act, consent given by a data principal must be free, specific, informed, unconditional, and unambiguous, and signified with a clear affirmative action.
[7] Section 4 of the DPDP Act.

employees for any purposes related to their employment. However, each of the personal data sets being collected must be aligned with and necessary for the purposes identified.

(iii) It is also important to note that the exemption provided for consensual collection of personal data is for all employment purposes. The DPDP Act does not limit the ambit of such exemption to only traditional employer-employee relationships. Some of those relevant situations could be:

1. An employer has outsourced certain functions (*background verification, processing payroll and management, providing insurance benefits etc.*) to third-party service providers. It is still pertinent to note any such outsourced functions entailing data processing must be based on a legitimate and valid contractual arrangement between the employer and the third-party service provider.[8]
2. An employee is transferred from one affiliate entity to another affiliate entity.

The above exemption is a significant deviation from the current data protection regime, which requires employers to obtain express consent before collecting sensitive personal information.[9] There are, however, certain aspects that certainly need to be clarified further.

d. **OBLIGATIONS OF EMPLOYERS AS DATA FIDUCIARIES**

(i) Some of the key obligations of employers under the DPDP Act as data fiduciaries have been discussed below:

1. Ensure compliance with the DPDP Act in respect of personal data processed by them or by a third party (*data processor*) on their behalf.[10]
2. Ensure personal data of the employees is accurate and complete, where it is used for decision making or is likely to be disclosed to another data fiduciary.
3. Implement appropriate organizational, technical measures (*reasonable security safeguards*) to protect personal data in its possession or under its control and comply with the DPDP and rules under it.
4. Duly notify the Data Protection Board of India ("**Board**") established under the DPDP Act as well as the affected data principals in the manner as may be prescribed subsequently, in the event of a data breach incident.
5. Appoint a Data Protection Officer and publish their details as per the requirements under the DPDP Act.
6. Establish an effective mechanism for the redressal of its employees' grievances.

(ii) ***Good Practices***: In addition to the above key obligations, it may also be a good practice to ensure that all processing activities relating to employees (*irrespective of whether any prior consent or notice requirements are applicable*) are recorded across internal policies or employment contracts (*i.e., documents which are generally accessible to employees*), given that employees are also entitled to a general fundamental right to informational privacy. Lastly, employers may also conduct sensitization trainings, and vertically applicable trainings (*this is particularly important since employees are often the biggest sources of data leaks in an organization*).

[8] Section 8(2) of the DPDP Act.
[9] Under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, sensitive personal information has been defined to include: (1) password, (2) financial information, (3) physical, physiological and mental health condition; (4) sexual orientation; (5) medical records and history; (6) Biometric information; (7) any detail relating to the above clauses as provided to body corporate for providing service.
[10] Since the ultimate responsibility to ensure compliance with the DPDP Act on the part of third-party processors would be on the employer, it is important that any third-party processing is based on a valid and robust contract. This is also a requirement under Section 8 (2) of the DPDP Act.

3. PENALTIES UNDER THE DPDP ACT

(i) The Board is responsible for inquiring into violations or non-compliance with the provisions of the DPDP Act. Under the DPDP Act[11], the Board is required to consider several factors while determining the amount of monetary penalty to be imposed, such as nature, gravity, and duration of the breach, its impact on the personal data of the data principal, whether the offender has realized a gain/avoided loss through such breach, efforts made to mitigate the effects of the breach, and the proportionality etc.

(ii) Monetary penalties under the DPDP Act are exponentially higher. For example, failure to implement reasonable security safeguards to prevent breaches of personal data could result in a penalty of up to INR 250 crore (*USD 30 million*). Further, a general penalty for breaches of other provisions of the DPDP Act may extend up to INR 50 crore (*USD 6 million*). Multiple contraventions could lead to even higher penalties as there is no cap on monetary penalties. In certain instances where a data fiduciary has been penalised in two or more instances, the Board can make a reference to the Central Government for blocking access by the public to any information generated, transmitted, received, stored or hosted by or in relation to such data fiduciary, in the interest of the general public – which in turn could restrict such data fiduciary from carrying on its business in India.

4. CONCLUSION

(i) India's data protection has now undergone a paradigm shift. While this is certainly a step in the right direction, it is likely that the compliance obligations of data fiduciaries will entail revisiting current practices and rethinking the need for collecting large amounts of personal data. It is important for employers to start evaluating and analysing their processing activities, internal practices and policies and contractual arrangements to identify gaps and ensuring compliance.

(ii) There may be situations in which an employer may not be able to use the exemption of legitimate use for processing employees' personal data. To address such situations, it is certainly worthwhile to execute employment agreements with employees that contain certain specific language around the collection of data.

(iii) In situations wherein an employer outsources certain employment-related functions to third parties, it would be prudent for them to evaluate the latter's internal safeguards, protocols as well as obligations of confidentiality to ensure that the personal data provided will always be adequately protected.

[11]Section 33(2) of the DPDP Act.

Authors: Vaibhav Bhardwaj | Shreya Suri | Ivana Chatterjee | Animay Singh

Date: December 21, 2023

Practice Areas: Employment | Data Privacy

DISCLAIMER