SCC ONLINE TIMES
Bringing you the Best Analytical Legal News

Digital Personal Data Protection Act, 2023: A Ready Reckoner for Employers

by Avik Biswas*, Supratim Chakraborty**, Sumantra Bose*** and Ivana Chatterjee****

Published on November 11, 2024 - By Bhumika Indulia

Post

Introduction

After several years of deliberation and legislative consultation, the Digital Personal Data Protection Act, 2023 (DPDP Act) received the President of India's assent on 11-8-2023. The Government is yet to notify the effective date of the legislation. While the common sentiment in the industry is that the DPDP Act only significantly impacts the information technology (IT) and information technology enabled services (ITeS) sector, it is undeniable that the DPDP Act is industry agnostic and impacts every entity that comes within the ambit of the applicability of the DPDP Act (i.e. processes personal data).

An employer, across sectors, shapes and sizes, collects a significant amount of personal data from its employees as well as potential employees/job seekers during the lifecycle of their employment. Such personal data may be collected during the employee selection and interview process for conducting background verification of the employees, during the employee onboarding process, for processing their payroll, undertaking statutory compliances as well as during employee separation. Further, even during internal disciplinary proceedings, many a times employers are required to collect personal data of their employees for purposes related to investigation and disciplinary proceedings.

To help employers navigate the intricacies of the DPDP Act and the additional compliances that they may be required to undertake, we have answered certain key questions in this article that are being discussed and debated in the human resource (HR), legal and compliance fraternities.

Frequently asked questions

(a) What type of data does the DPDP Act apply to? Does it apply to the information that an organisation collects from its employees?

The DPDP Act applies to the processing of any kind of personal data in digital form. Personal data would be data that can identify an individual. This would include their name, address, contact information, identity proof, etc. An organisation would collect several such categories of personal data from employees during their cycle of employment. Therefore, compliance with the DPDP Act is required for processing personal data collected by an organisation from its employees, in the capacity as a "data fiduciary".

> **Did you know?** An employee's data such as their bank account number, financial statements, IT returns, educational qualification documents, address proof, biometric information (fingerprint, retina scan) qualify as personal data under the DPDP Act.

Under the DPDP Act, a data fiduciary is defined as any person who determines the purpose and means of processing of personal data. As an employer, it will also be important to monitor the activities of data processors as all penalties under the DPDP Act are with respect to data fiduciaries. Further, employers would also be required to abide by any restrictions on transfer of personal data to countries as may be notified by the Central Government.

> **Did you know?** If an employer outsources its payroll operations to a third-party service provider, the employer would be the data fiduciary, and the payroll service provider would be the data processor under the DPDP Act.

Therefore, all obligations under the DPDP Act would be on the employer in their capacity as the data fiduciary. Employers need to ensure that it mandatorily has a

contract in place with the payroll service provider (who would be the data processor) clearly mentioning the data processing related rights and obligations.

(b) Does an organisation need to obtain consent from its employees each time it processes their personal data?

The DPDP Act provides for certain legitimate uses as a ground of processing personal data where consent is not required. One of these is based on the purposes of employment or those related to safeguarding the employer from loss or liability such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, or provision of any service or benefit sought by an employee. Therefore, consent would not be required from an employee if processing of personal data is due to the abovementioned reasons. However, organisations will still be subject to other obligations under the DPDP Act as a data fiduciary. Additionally, it is not clear if the legitimate use ground can be used during recruitment or for optional events for employees (such as company organised family day). Therefore, consent may still be required in such cases.

(c) Will employees be considered as data principals under the DPDP Act? What are the rights of employees under the DPDP Act?

Under the DPDP Act, a data principal is defined as an individual to whom the personal data relates. Therefore, if personal data is collected from employees, they will be considered as data principals and the employer will be a data fiduciary.

Under the DPDP Act, data principals have certain rights depending on the grounds of processing. These rights include the right to grievance redressal and to nominate a person to exercise rights on their behalf in case of death or incapacity. If consent is used as a ground of processing, data principals have certain additional rights of access and rectification of personal data. Therefore, for employers, it is important to keep personal data of employees properly recorded and mapped to the relevant ground of processing.

Did you know? Under the DPDP Act, an employer may be required to give access to a third party to an employee's personal data if such employee nominates such party to exercise the employee's rights under the DPDP Act upon their death or incapacity.

employee could nominate any third party to access,

(d) What are the obligations of employers as data fiduciaries under the DPDP Act?

As data fiduciaries, a few of the key obligations of employers under the DPDP Act are:

(*i*) Ensuring that the personal data of its employees are complete and accurate in situations where such data is used for decision-making or in situations where such personal data is likely to be disclosed to other data fiduciaries.

(*ii*) Exercising caution and ensuring compliance with the DPDP Act regarding the personal data being processed by them or by an external party (data processor) on their behalf.

(*iii*) Implementing appropriate reasonable technical security safeguards and other organisational measures to protect the personal data that is in its possession and control.

(*iv*) In case of a data breach incident in the organisation, notifying the Data Protection Board of India established under the DPDP Act as well as the affected data principals.

(*v*) If the employer is categorised as a "significant data fiduciary", appointing a Data Protection Officer and publishing such officer's contact details. Employers not being categorised as significant data fiduciaries may appoint an officer of a similar stature.

Note: The Central Government may categorise certain data fiduciaries or classes of data fiduciaries as "significant data fiduciaries" based on various factors such as the volume and sensitivity of personal data processed, the risk to the rights of the data principal and the potential impact to the sovereignty of India, amongst others.

(*vi*) Establishing an effective grievance redressal mechanism for its employees.

> **Did you know?** Many employers allow their employees to annually rectify/confirm the accuracy of the personal data they have shared with the organisation.

(e) Will an organisation need to make changes to its internal policies, standard employment contract to align itself with the DPDP Act?

As a first step, it is important for employers to internally evaluate their compliances under the DPDP Act and its corresponding rules (once enacted). Employers should review its existing policies and practices with respect to data privacy, data processing and data retention, and align them with the requirements under the upcoming law.

> **Best practice:** Employers are enacting standalone Employee Data Protection Policy for their employees.

(f) Does the in-house legal team and/or HR team have any duties or role to play under the DPDP Act?

While the DPDP Act does not specifically impose any roles and responsibilities on the members of the Legal Department members and/or HR personnel, such officials should nevertheless ensure that: (*i*) the internal policies and documents of the organisation are compliant with the DPDP Act; (*ii*) the employees handling personal data within the organisation are adequately sensitised on the provisions of the DPDP Act to prevent any incident of data breach within the organisation; and (*iii*) conduct periodic internal assessments to assess the organisation's compliance with the DPDP Act and the impact that the processing of personal data has on the data principals.

Best practice: Employers are proactively conducting training sessions for employees with respect to their roles and responsibilities under the DPDP Act. Further, employers are also evaluating the policies and practices of its business partners (with whom the employers have shared its employees' personal data) to significantly mitigate any risks and liabilities under the DPDP Act.

(g) Can an employer transfer its employees' data to its affiliate entity outside India?

Subject to certain terms and conditions, yes, an employer may transfer employee data to an affiliate entity outside India. The Central Government has the power under the DPDP Act to restrict the transfer to certain countries (which will be notified in due course). It is important to bear in mind that if any other applicable law imposes a high degree of restriction on an employer with respect to such transfer, the restrictions under such law will be applicable.

Did you know? While conducting internal investigations/disciplinary proceedings, certain employers transfer a significant amount of personal data to an investigation agency outside India. In such cases, employers will be required to comply with the DPDP Act.

Next steps

As immediate steps, employers should consider appointing a team that will be responsible for formulating/revising the relevant policies and implementing the necessary procedures and protocols, identifying gaps and ensuring compliance with the DPDP Act. Employers are also engaging external service providers with specific expertise to guide the internal team with the harmonisation process. Further, if an employer has outsourced a few of its employee-related operations and shared employees' personal data with such third parties, it is crucial for employers to revisit the contracts with such third parties to ensure that there are adequate data protection clauses in the agreement in the context of the DPDP Act.

While the DPDP Act is definitely a step in the right direction, it entails significant preparation on part of an employer before the legislation is brought into effect.

***Partner, Khaitan & Co.**

****Partner, Khaitan & Co.**

*****Counsel, Khaitan & Co.**

******Principal Associate, Khaitan & Co.**

Tags : compliance requirements | data fiduciary | data privacy | data processing | Data processor | data protection compliance | data protection regulations |

Digital Personal Data Protection Act | DPDP Act 2023 | DPDT Act employers guide | employee data security | employer obligations | employers' guide | Indian data protection law | Khaitan & Co | personal data

MOST READ

24 hours 7 days All time