Edutech sector and Digital Personal Data Protection Act, 2023 ("DPDP Act")

When it will be applicable?

The DPDP Act has received the Presidential assent and it will become applicable upon notification in official gazette by the Central Government. Different portions of DPDP Act may be enforced at different points of time.

WHAT ARE THE IMMEDIATE PLANS & ACTIONS?

The enactment for DPDP Act requires following immediate actions on part of data fiduciaries:

- ◯ Internal due diligence of data collection and data flow
- ◯ Evaluate the portions where direct consent from Data Principal is received
- ◯ Reviewing all privacy notices
- ◯ Review whether all data collected are required for purpose
- ◯ Formulate a plan to collect updated consent
- ◯ Re-design systems - Privacy First Model/ Privacy by Design Model
- ◯ Selection & training of Grievance Officers
- ◯ Mechanism for revocation of consent

What would be the Impact on EduTech?

- Data Handled by Ed-Tech sector: Ed-tech sector deals with personal data belonging to teachers, children and adults, and often their parents while using the education tools.
- No carve out: DPDP Act does not yet provide a carve-out for EduTech sector entities including schools, companies providing education services directly to students, companies providing education services through a school, etc. However, the Central government may notify for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations in relation to processing of children's data if the Central Government is satisfied that a Data Fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe. The Central Government may also prescribe certain classes of Data Fiduciaries who may be exempted from the said obligations for the specified purposes and subject to fulfilling the specified conditions. EduTech sector entities will have to act in compliance with the provisions of DPDP Act in relation to processing of children's data unless exempted by the Central Government.
- Seeking consent from parents or lawful guardian: The DPDP Act defines child as an individual below the age of eighteen years. For the processing of personal data of a child a Data Fiduciary is required to take the consent from the parents or lawful guardian of the child.

What would be the Impact on EduTech? Cont....

- Restriction under DPDP Act on Processing of children's data:
  The Data Fiduciaries shall not:
  1. undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child
  2. not undertake tracking or behavioral monitoring of children
  3. not undertake targeted advertising directed at children.

- Critical Issues:
  1. Tracking of the progress/ attendance of a student, which is common for educational tools, might be considered as behavior tracking, which may affect the functioning of educational tools.
  2. Applications which gamify education and have option for in-app purchases. EduTech entities allowing gamify education will have to be careful and ensure that these does not cause any detriment to children.
  3. Entities providing services to a school will have to ensure that the consent is procured by the school from the parents or lawful guardians.
  4. There may be an impact on school systems if behavioral tracking is not allowed.
  5. Marketing of Edutech tools may be considered as advertising directed at children.
  6. Using and controlling automated processing by AI and other modern means.

- Consents required:

1. Schools to to take parental consent if ed-tech tools are being used at the time of enrolment or before usage.
2. Ed tech companies to take parental consent of children using such tools.

- Significant Data Fiduciary obligations: Entities in EduTech sector may be designated as significant data fiduciaries based on the volume and sensitivity of personal data that is being processed, risks to end users who are mostly children and its impact on the sovereignty, integrity and security of the nation. If so designated, they will then have to undertake additional compliances and obligations such as appointing a resident data protection officer, appointing an independent data auditor, data localization requirements, conducting periodic data protection impact assessments, and conducting periodic audits.

General Impact?

- Employee and Vendor data: Employee data includes personal details including, ID numbers, health data, financial details, payroll, and health insurance collected for payroll processing, for checking the performance of the person, for hiring, workforce planning, performance management, training, and development, workplace safety, employee communications, compliance with laws, leave and time off management, emergency contact, security purposes, retirement planning, workplace diversity and inclusion, human resources management and taxation, etc. It is necessary to procure general consent from candidates during the hiring process and later data collection and processing clauses should be added to the employment contract. Further, specific consent should be sought from the employees for employee surveys, and marketing/ non-essential communications, when processing their sensitive personal data. Vendor consent will be required as any other data principal.
- Past data compliance: The DPDP Act does not have a retrospective application but in cases of data collected in the past, where consent for the processing of data has been obtained from the data principal before the enactment of the DPDP Act, the requirement for giving notice under DPDP Act must be fulfilled and consent is required to be sought again. Data fiduciaries are required to provide an itemized notice in accordance with the DPDP Act to the Data Principal and describe what personal data has been collected and the purpose of processing. The data collected before the notification of the DPDP Act will be subjected to the provisions of the DPDP Act from the date of commencement of the DPDP Act.
- Data Processor and Data Fiduciary agreements: Fiduciary and processor obligations under data processing agreements will include obligations implementing appropriate measures to protect the security of data, including encryption and pseudonymization of data if appropriate, ensuring data confidentiality, integrity, and resilience and process for regularly testing, assessing, and evaluating security.

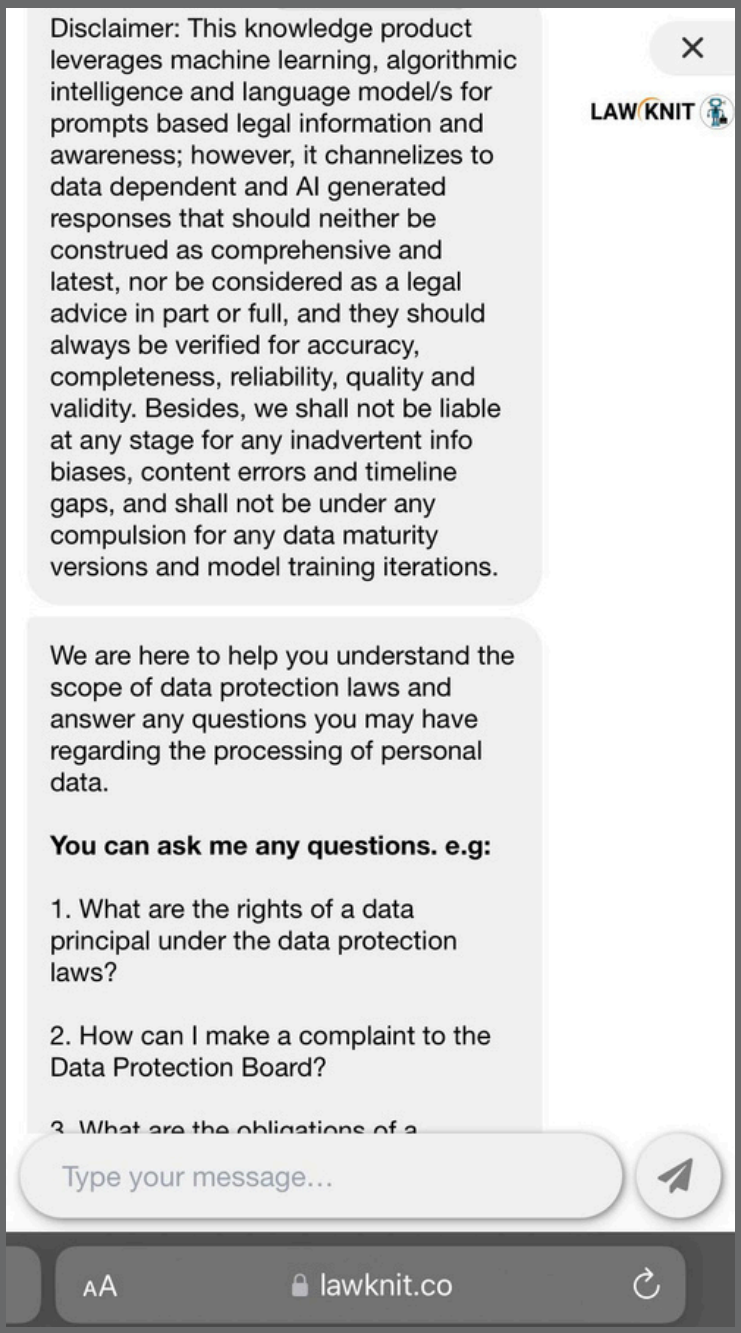
How can we help?

We can assist the Fintech entities with the following:

- Conducting Gap Analysis with the current format of the organization
- Advisory and assisting in implementation by organizations
- Providing documentation assistance in relation to Data Processor and Data Fiduciary agreements, consent mechanisms

KNIT-KNOW-AI

LAWKNIT KNOWLEDGE ASSISTANT



The Digital Personal Data Protection Bill, 2023 was passed in Parliament and received presidential assent on August 12, 2023. The Digital Personal Data Protection Act, 2023 ("DPDP Act") is applicable to the processing of all kinds of digital personal data within India irrespective of data being collected online or offline. It is also applicable to the processing of personal data outside India if it is for offering goods or services in India. The Act also grants certain rights to individuals which includes the right to seek correction and erasure, obtain information and grievance redressal mechanism. Some of the details of DPDP Act is as follows for further feel free to access our DPDP AI- KNIT KNOW-DP

For Queries reach out to us:
Clients: Create query on LawKNIT platform

Non-Clients: write to us
arunabh@lawknit.co

LAWKNIT