

Education Sector Hotline

October 11, 2021

THE CALM BEFORE THE STORM: HOW THE UPCOMING DATA PROTECTION LAW WILL IMPACT EDTECH IN INDIA

The past few years have seen an EdTech boom in India. Some say that this is just the start – and much more is yet to come. As per latest numbers, Indian born and bred Byju's is valued at USD 18 billion,¹ making it the highest valued Indian start-up. Several EdTech start-ups have already joined the Unicorn club, and many more are in the waiting. This is an indicator of the size and growth trajectory of EdTech in India. Especially with parents and children stuck at home, the pandemic allowed EdTech especially online learning platforms, to grow in leaps and bounds.

As EdTech entities are primarily technology driven, they fall outside the purview of education laws *per se*, allowing business flexibility. However, this is not to say that they function in a regulatory vacuum. There is a host of other laws that apply to them. One of them being the Information Technology Act, 2000 (**IT Act**) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**") which are the current "data protection" laws in India. India is also in the process of enacting the *Personal Data Protection Bill, 2019 (PDP Bill)* as law, which is set to overhaul the current data protection framework in the country in the (hopefully) near future.²

What is the implication of not paying heed to data laws? We don't have to look very far to see the fallout from taking data protection regulations lightly - Google and YouTube were fined USD 170 million by the Federal Trade

Commission in America for violations of the children's privacy law in 2019.³ TikTok is facing a lawsuit for alleged violations in their use of children's data in the UK.⁴ Similar to Europe's General Data Protection Regulation, the PDP Bill prescribes hefty fines in cases of non-compliance – ranging up to 4% of global turnover or INR fifteen crore (approx. USD 2 million); and criminal penalties in limited cases. With these risks in mind, time is of the essence for our homegrown EdTech platforms to consider data protection and data collection practices seriously and get their house in order.

Generally, EdTech entities and platforms collect a significant amount of data while offering their services. As an example, when a student sets up their profile on an e-learning website, the platform collects their name, contact details, passwords, age, identification, gender, qualifications, *et al.* They may also collect similar details about the student's parent or guardian. While we don't mean to generalize, there are also a large number of EdTech platforms who monetize such data through data analytics and data transfers. They may use this data for internal business planning purposes - to track traffic, user engagement etc., for targeted marketing and at times, share it with associated or partnering entities to position their product or services to prospective customers. This data could also be used for targeted marketing specially on social media. In this digital age, where so much of our lives is tracked by devices, it is essential for all stakeholders in the education system – be it EdTech platforms, schools, teachers and even parents to realize the importance of data, how it is collected, what is it collected for, what is it used for, especially children's data, as this could have implications on what a child consumes on the internet, for example through targeted or sponsored advertisements or otherwise. Personal data, especially that of minors, should thus only be shared consciously.

The collection of this data and its use will soon be subject to stringent data protection laws in India. What is the current law, and what is the PDP Bill, and what do they say about data protection and privacy? We explain below.

CURRENT DATA PROTECTION LAW: ARE YOU COLLECTING SENSITIVE PERSONAL DATA?

- **What is kind of data is covered under the current data protection law?** IT Act and SPDI Rules recognize two forms of data:
 - **Personal Information ("PI")**: which is defined as "*any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person*". PI includes data such as name, contact details, age, etc.
 - **Sensitive personal data or information ("SPDI")** which consists of the following items of personal information which can identify a natural person: *password; financial information such as Bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; and biometric information.*
- **Who does the law apply to?** There are no specific compliance requirements for the processing of PI, though certain penal provisions may apply in the event of unauthorised disclosure. The SPDI Rules prescribe limited compliance requirements for an entity located in India that collects, stores, processes, receives or otherwise handles SPDI, such as to take consent from user for data collection and use, give notice of collection of data, adopt

Research Papers

Little International Guide (India) 2024

November 08, 2024

Unmasking Deepfakes

October 25, 2024

Are we ready for Designer Babies

October 24, 2024

Research Articles

The Bitcoin Effect

November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!

September 15, 2024

Navigating the Boom: Rise of M&A in Healthcare

August 23, 2024

Audio

Digital Lending - Part 1 - What's New with NBFC P2Ps

November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I

August 26, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part II

August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FIH event in Riyadh

October 31, 2024

Analysing SEBI's Consultation Paper on Simplification of registration for FPIs

September 26, 2024

a privacy policy, appoint a grievance officer to redress data related issues, and undertake and adopt reasonable security procedures and practices for the information, to name a few.

- **Are there any limitations on processing or profiling of data?** Yes, consent is necessary for any such processing or profiling that includes SPDI. However, as SPDI is of limited forms, and the data collected by EdTech companies is usually in the nature of PI, for which there are no express limitations on such processing under current data protection law. Thus, if the data processed does not qualify as SPDI, current law does not mandate parental consent before collecting such data, nor does it place any restrictions on profiling or analyzing minor's data for targeted advertisements. This may shortly change once the PDP Bill is passed. We explain more below.

THE PDP BILL: NOT TO BE TAKEN LIGHTLY

A few provisions of the PDP Bill of significance to EdTech are:⁵

- **Extraterritorial applicability:** As compared to the current law being applicable only to Indian entities, the PDP Bill would apply to entities located outside India collecting personal data if certain nexus requirements are met.⁶
- **Compliance requirements for all personal data:** The PDP Bill significantly widens the net of compliance, and will prescribe compliance requirements even for entities who process personal data not amounting to SPDI, such as a name, contact information, age, etc. To name a few compliance requirements, entities will need to take consent, give notice, provide for data protection rights, and institute security safeguards for the collection of all personal data.
- **Data localization for sensitive data:** A copy of all 'sensitive personal data' must be stored in India but may be transferred outside India. 'Critical personal data' (which will be defined by the Central Government) must be processed only in India, with exceptions. A vast majority of entities store data offshore. This will now change and organizations processing sensitive personal data and critical data will need prepare their infrastructure for data localization.
- **Cross-border transfer restrictions:** Mere personal data (that is non sensitive personal data or critical personal data) has been exempted from cross-border transfer restrictions. Sensitive personal data may be transferred outside India only if certain compliance requirements are met. This would be relevant for companies transferring data to their group companies and affiliates located offshore.
- **Data breach notification:** We hear of data leaks and data breaches often. Current law does not prescribe for a data breach notification for data breaches involving PI. Under the PDP Bill, the soon to be formed Data Protection Authority is to be intimated in case of a data breach. This authority may require the entity to report the data breach to affected individuals and certain remedial action be taken.
- **Hefty penalties including global turnover:** The PDP Bill provides for civil compensation; financial penalties such as fines (up to 4% of global turnover); and criminal penalties in the limited case of unauthorized deidentification of data. This is significant as the global turnover of companies having offshore entities may be significantly high.

Most significantly, the PDP Bill also prescribes for safeguards in the processing of minor's data, as well as provisions that would impact EdTech platforms and their advertisement based revenue streams. These are as follows:

- **Age of consent:** The PDP Bill mandates that parental consent will be necessary for the processing of personal data of children (i.e., persons below the age of eighteen years). There are certain platforms which are targeted / focused on young adults aged 14-18 such as casual gaming, education, or even specific video platforms. Given how tech and mobile savvy children in this age group are, seeking parental consent for the collection of all forms of data could turn out to be an uphill task. Hence, pragmatic business solutions are needed to meet this requirement.
- **Age Gating and Verification Obligations:** Under the PDP Bill, EdTech platforms will soon need to verify the age of children before processing their personal data.⁷ Thus, the obligation to ensure age gating / verification and the necessary tools will have to be implemented by businesses, and will need to be worked into the functioning of online platforms. Age verification mechanisms will be specified by regulations.
- **Bar on Profiling/Behavioural Monitoring/Targeted Advertisements:** Platforms or businesses who operate commercial websites / online services directed at children; or process large volumes of personal data of children will be notified as 'Guardian Data Fiduciaries' once the PDP Bill is enacted. Such 'Guardian Data Fiduciaries' are barred from undertaking activities such as profiling, tracking, behavioural monitoring, or targeting advertising directed at children, or any form of processing that could cause significant harm to children. As an example, audio / video streaming platforms may not be able to offer suggestions on "what to watch" or show "relevant advertisements" based on individual preferences. This could mean tweaks in business models and structures for compliance with the new law.

The PDP Bill is due to be re-introduced in Parliament in November-December 2021. Albeit there has been some delay, a robust data protection law will surely be introduced in India. While the easiest solution would be to wait and watch for the next version of the law, it may be prudent for EdTech platforms to use this lead time to examine their data collection and processing practices in order to be future ready. The proposed law is based on global practices, and will surely help EdTech platforms in global level compliances. Even if data related compliances for a variety of data are not legally required at the moment, EdTech platforms can take inspiration from multinational companies who have begun to get their systems in order. Apart from EdTech platforms themselves, it would serve parents, teachers and educational institutions well to also educate themselves on their rights with respect to data privacy and processing, and possible redressal mechanisms in case of privacy breaches for children. This will ensure a safe and secure digital environment for our future generation.

¹ <https://techcrunch.com/2021/10/04/indian-edtech-giant-byjus-valued-at-18-billion-in-new-funding/> (Last accessed October 8, 2021).

² The PDP Bill is currently under consideration by a Joint Parliamentary Committee, which is slated to meet in October 2021 to study the PDP Bill.

³ <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations> (Last accessed October 8, 2021).

⁴ <https://www.bbc.com/news/technology-56815480> (Last accessed October 8, 2021).

⁵ You may read further about the PDP Bill in our research paper available at: https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Privacy-and-Data-India_s-Turn-to-Bat-on-the-World-Stage.pdf (Last accessed October 8, 2021).

⁶ The PDP Bill is designed to have extra-territorial application and is linked to the processing of personal data by entities not present within the territory of India; if such processing is *"(a) in connection with any business carried on in India, or any systematic activity of offering goods or services to Data Principals within the territory of India; or (b) in connection with any activity which involves profiling of Data Principals within the territory of India"*.

⁷ The only entities exempted from the parental consent requirement are those guardian data fiduciaries who provide exclusive counselling or child protection services.

DISCLAIMER

The contents of this hotline should not be construed as legal opinion. View detailed disclaimer.

This Hotline provides general information existing at the time of preparation. The Hotline is intended as a news update and Nishith Desai Associates neither assumes nor accepts any responsibility for any loss arising to any person acting or refraining from acting as a result of any material contained in this Hotline. It is recommended that professional advice be taken based on the specific facts and circumstances. This Hotline does not substitute the need to refer to the original pronouncements.

This is not a Spam mail. You have received this mail because you have either requested for it or someone must have suggested your name. Since India has no anti-spamming law, we refer to the US directive, which states that a mail cannot be considered Spam if it contains the sender's contact information, which this mail does. In case this mail doesn't concern you, please unsubscribe from mailing list.