How will India's Personal Data Protection Bill, 2019 impact schools?

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the ninth article in the series. Read our extensive coverage of the Bill here.

By Rahul Narayan

As thousands of anxious parents are busy filling forms for school admissions, and all the schools are engaged in the mammoth yet intricate task of sifting through thousands of forms to find "suitable candidates for admission", it is a truth that needs to be universally acknowledged that the system works on the principle of "*give me your data and I will give you … admission*". Indeed, in the entire school journey from admission to graduation to alumni, schools collect data, store data, process data and generate data.

What kind of data do schools collect?

At admission, schools typically ask for names, ages, addresses, photographs, sex, religion, Aadhaar numbers[#], birth certificates, details of siblings, parents' names, parents' qualifications, family income, telephone numbers, email addresses, etc. Once children are admitted, financial data such as bank account details, and health data such as blood group, allergies, weight, height, immunisations, regular medication (if any), dental check-ups, eye check-ups, etc. are added. Then there are progress reports, participation details, and disciplinary records of students which are generated by schools. Finally, there are contact details and achievements of alumni which are kept, in particular, for school fundraising, directories, even advertising, etc.

At every stage, schools collect and process personal data including sensitive personal data — financial data and health data —of their students *and* of their parents/guardians. **Consequently, the Personal Data Protection Bill ("the Bill") has enormous ramifications for schools.**

How will the Bill classify schools?

There can be little doubt that schools are "data fiduciaries" for the purposes of the PDP Bill and as such, they are required to fulfil all obligations under Chapter II, that is, Sections 4 to 11, particularly those dealing with purpose limitation, the requirement of consent, etc., as well as the accountability and transparency measures specified in Chapter VI. Since schools inevitably process large volumes of personal data of children, they will also be regulated as guardian data fiduciaries for the purpose of Chapter IV of the PDP Bill and the regulations made under them. Considering the volume and sensitivity of

personal data processed, the Data Protection Authority (DPA) may also seek to regulate schools as Significant Data Fiduciaries under Section 26 of the Bill. Government run schools may also be regulated differently if they are classified as a "service provided by a government" under Section 12(a)(i) of the Bill.

Schools, like other data fiduciaries, will thus be required to prepare a "privacy by design" policy dealing with practices and systems to anticipate, identify and avoid harm to the students or former students, ensure technological processing is in accordance with certified standards, and to ensure that the processing has to be secure at all stages. They also have to comply with the requirements for transparency in processing, and for data security. If schools are classified as Significant Data Fiduciaries, they will be required to appoint Data Protection Officers, carry out data protection impact assessments in case they process data through new technology, and maintain records and carry out annual data audits.

What does all this entail in terms of how schools operate? Quite a lot actually. Consider the following questions as a kind of sample of what needs to be tackled:

Will schools have to change the way their admission forms are drafted and processed?

Simply put, yes they will — both in terms of content and in terms of processing.

Content of admission form:

1. **Purpose limitation:** In terms of data required, forms will have to be limited to data that is connected or incidental to the "specific, clear and lawful purpose" of ensuring admission to an educational institution. The notification dated January 6, 2016issued by the Department of Education already regulates what can be asked this to a large extent though this has been challenged before the Delhi High Court (W.P. (C) No. 448/2016) and awaits a final decision. It is pertinent to note that admission cannot be denied or made conditional on consent to processing of any personal data not necessary for admission.
2. **Taking consent:** The form will also have to explain in simple and easily comprehensible language(s) the nature and categories of personal data collected, the duration of time such data is stored, the identities of whomsoever such data may be shared with, details of the rights and remedies available to the persons whose data is collected, the procedure for grievance redressal, etc. The essential requirement is the free, informed, specific, and clear consent that may be withdrawn. **The burden of showing that the consent taken was informed consent rests upon the schools.**
3. **Separate consent for sensitive personal data:** Since some of the data collected will be sensitive personal data (such as health and financial data), the form will be explicitly required to inform the parents/guardians in clear terms the purpose of or operation in processing that is likely to

cause significant harm. The parents will also have to be given a choice of separately consenting to different categories of sensitive personal data.

- Government schools provide a service from the state and thus may be exempt from some of the rigors of obtaining consent as distinct from private schools. However, the boundaries of such exemption are unclear under section 12(a)(i) of the Bill.

Processing of admission data:

1. **The school is responsible for compliance with the requirements of the PDP Bill for any processing that is carried out on its behalf.** This would entail an overhaul of the mechanisms currently used to process applications. If data processors are hired, they will need to be monitored to ensure compliance. Such data processors may only be appointed vide a contract and are bound by the instructions of the Data Fiduciary and must treat data as confidential as per Section 31 of the Bill.
2. Schools would also need **a policy to destroy or delete such data collected at the end of the admission process** and set up a time frame in this regard erring on the side of lesser rather than greater time of retention. Applications that do not lead to a successful admission ought not to be kept beyond a reasonable time frame following the draw of lots. For successful candidates, such data as is required by law must be maintained. For retention of other data for any purpose, explicit consent of the parents/guardians will be necessary.
3. Policies framed for data processing, data retention and data destruction will have to take into account that **there is a general obligation that personal data of the child is to be processed in a manner that protects the rights of the child and which must be in her best interest.** Schools, as likely guardian data fiduciaries, shall be barred from profiling, tracking, or behaviourally monitoring of children or undertaking any processing that can cause significant harm to the child.

Can schools share sensitive personal details of children such as health data?

Usually they cannot —especially not without the consent of the parents or guardians in case of minors. As a guardian data fiduciary, schools have an additional duty to avoid processing of personal data that can cause significant harm to the child.

However, an explicit exception is made to respond to a medical emergency involving a severe threat to the death of the individual or to provide treatment or services during an epidemic or threat to public health, as per Section 12(e) of the Bill.

How must schools deal with data they generate — such as performance records, report cards, etc?

School report cards, performance reports, and suspension letters all fall in the category of personal data. As such, they cannot be shared without prior explicit consent except for specific and limited grounds contained in Sections 12 and 13 of the PDP Bill. Sharing of data with the education boards, for example, will probably be mandated. Sharing data in case of transferring students would usually happen with the consent of the parents of the transferring children. However, there are aspects of this that are tricky. What happens if the parents want deleted reference to disciplinary inquiries or issues like bed wetting from the records?

Under section 9 of the Bill, students, as data principals, have the right to ask for erasure of personal data that is no longer necessary for the purpose for which it was created. This would cover old disciplinary records or performance certificates. Schools have the right to refuse to do this if they have adequate justification which they explain to the Student. If the student is dissatisfied with the justification, she has the right to insist that the data contains a caveat that it is disputed by the student.

Students may also argue that such data processing may cause significant harm or amounts to profiling, tracking or behavioural monitoring, which are expressly barred for guardian data fiduciaries such as Schools under Section 16(5) of the Bill at the risk of penalties under Section 57(2)(b). It is not a stretch to see that performance records, report cards and the like could be construed to be data that amounts to profiling, tracking or behaviourally monitoring of children, particularly when such data is compiled on an annual basis.

Until Regulations under section 16(6) are framed, it would be difficult to see how schools are to deal with this. **This broad ban under Section 16(5) makes sense for guardian data fiduciaries that deal with e-commerce or gaming, but is overbroad and even counter-productive for educational institutions such as schools that ought to track, profile, or monitor at least some of what children are up to with a view to enhancing the educational experience.** Should schools be able to monitor what websites children go to when they use school computers? Should teachers be able to profile kids being considered for scholarships or those that may be at risk? Under Section 16(5) of the Bill, they cannot.

Regulations by the Data Protection Authority under Section 16(6) may modify their applicability for data fiduciaries that offer "counselling or child protection services to the child" though schools may need a broader carve out for traditional pedagogical functions. Rather than a broad ban and a narrow exception, the contours of which will be decided by regulation, it may be more prudent to exempt schools and educational institutions with respect to their activities related to learning or welfare while banning profiling or tracking that is linked to say religion or race or sexuality.

Students and former students have, in addition to other rights, the right to be forgotten to prevent disclosure of personal data under Section 20 of the Bill. This right can be exercised subject to the order of an adjudicating officer who must balance this right with the right to free speech and expression and keeping in mind, for example, the role of the former student in public life.

Conclusion

Data protection and its relationship with the ancient right of privacy have been debated and argued in the developed world since at least the 1970s. Principles have evolved and developed organically, frequently from bottom up. In India, however, this dialogue only really began after the Supreme Court re-affirmed the right to privacy in *Puttaswamy I* and dealt with the Aadhaar Scheme in *Puttaswamy II*. The PDP Bill, when enacted, will be the first significant data protection act in India. We don't have much past practice or experience to guide us how to interpret the broad principles the Bill identifies. What final principles end up being adopted will depend on many factors such as the composition of the data protection authority, the enforcement of the rights conferred by the bill and most of all by industry practice and regulations.

For schools, many ticklish practical questions relating to data protection will need to be ironed out, in particular because of the quality and quantity of data they collect of children. Would data of children have to be anonymised to even higher specifications than data of adults to prevent any possible use that could lead to significant harm in case of government request for data? To what extent are schools permitted to share student data with colleges when the latter request the former for verification? What happens when verification requires sensitive personal data to be transferred out of the country? How will the restrictions imposed on checking student behavioural patterns be interpreted by the data protection authority and by the courts? Can school teachers use examination results and other records to offer tuition to students? Do alumni directories violate the principles of data protection? Can schools use parents' financial information to solicit funds?

Schools will need to be schooled.

This is specifically barred under the *Puttawamy II* judgment.

*

Rahul Narayan *is an Advocate-on-Record in the Supreme Court of India. He has appeared in matters involving the right to privacy, access to internet, intermediary liability and digital rights. He also advises companies and institutions on issues relating to compliance with technology law, and cyber frauds. He can be reached at Rahulnarayan@lawfirst.in.*

Edited by Aditi Agrawal