7 ASPECTS TO REMEMBER ABOUT CHILDREN DATA PRIVACY UNDER THE NEW DATA PROTECTION REGIME

WEDNESDAY WISDOM

21-01-2026

Introduction [1]:

Have you ever wondered that when children spend time online, how they end up sharing data with Apps unknowingly? Booking a cab or auto involves location sharing, ordering food or products online again involves sharing of preferences and sometimes health conditions as well. Voicing out one's opinion on any social media again involves sharing personal views.

Analysis of this data can sometimes help build a very distinct result at the backend. An interesting example was in news few years ago, when an AI model analyzed the buying and scrolling pattern of a girl, and concluded that she was pregnant. When the store started sending discount coupons related to baby clothes, the family was shocked.[2]

Well, is that the price that parents and children are paying for using digital ecosystem -from AI-driven learning analytics and personalized education tools to behavior-based gaming algorithms?

The Digital Personal Data Protection Act, 2023 (DPDP Act) and the Rules framed under the DPDP Act and notified in November 2025 (DPDP Rules), are enacted by the Indian Parliament essentially to safeguard privacy of individuals with one of its focuse on protection of children privacy. Children' right to privacy is well recognized internationally as well[3]. Article 16 of the Convention of the Rights of the Child clearly indicate that no child shall be subjected to arbitrary or unlawful interference with his or her privacy[4].

While innovation in child-centric technology is often framed as empowerment, the legal questions around data collection, processing are far more complex and this article examines seven key questions about the special provisions of data protection applicable to children and the possible consequences of any data breaches.

[1] The article reflects the general work of the author on the date of publication and the views expressed are personal. No reader should act on any statement contained herein without seeking detailed professional advice.
[2] How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did
[3] Article 17 of the Universal Declaration of Human Rights, recognizes individuals' right to privacy.
[4] Convention on the Rights of the Child | OHCHR

- **Who is a child?**

Section 2(f) of the DPDP Act defines a child as an individual who has not completed the age of eighteen years. This definition is distinct from GDPR which defines a child as below 13.

- **What would be considered as personal data of the child?**

The definition of data is very wide and may include "data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means.

"personal data" means any data about an individual who is identifiable by or in relation to such data.

"personal data breach" means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data;

So personal data of a child could mean directly identifiable data like the photographs, names, identity details or photographs of the school identity cards or admit cards, marksheets, or even indirectly identifiable data (which can be clubbed together to identify a person)- like child of A and B, child living in a specific address, child with a specific passport number.

Accordingly, data breach could mean sharing of such personal data with people who are not authorized or entitled to receive them. For example, if a child wins a particular competition, his/her photograph with the trophy can be used by such schools or institutes which have the proper consent for using it.

- **What are the obligations of data fiduciary (the one who collects personal data -DF) under DPDP Act with respect to a child' data?**

Section 9 specifies the below main obligations or restrictions on DF before processing any child's personal data:

1. Obtaining a verifiable consent of the parent or lawful guardian of such child;
2. Restriction on processing of personal data that is likely to cause any detrimental effect on the well-being of a child;
3. Restriction on tracking or behavioural monitoring of children or targeted advertising directed at children

- **What are the parameters of a verifiable consent?**

The parameters of a verifiable consent have been clarified under the DPDP Rules to an extent through some interesting provisions and indicate an approach of privacy by design. The DPDP Rules state that DF shall:

1. adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child; and
2. observe due diligence, for checking that the individual identifying herself as the parent is an adult who is so identifiable by reference to
    a. reliable details of identity and age of the individual available with the DF; or
    b. details of identity and age, voluntarily provided —
        i. by the individual; or
        ii. through a virtual token mapped to such details, which is issued by an authorised entity.

The DPDP Rules have also provided four interesting illustrations to understand this better.

C is a child, P is a parent, and DF is a Data Fiduciary. A user account of C is sought to be created on the online platform of DF, by processing the personal data of C.

Case 1:
C informs DF that she is a child and declares P as her parent. DF shall enable P to identify herself through its website, app or other appropriate means. **P identifies herself as the parent and informs DF that she is a registered user on DF's platform and has previously made available her identity and age details to DF**. Before processing C's personal data for the creation of her user account, DF shall check to confirm that it holds reliable identity and age details of P and that P is an identifiable adult.

Takeaway from this case study: The DF should adopt appropriate list of documentation on its platform to confirm necessary submission of documentation and maintain meticulous records of this documentation. Further, DF may also consider having a clear implementation strategy that enable its system to check that P is actually an identifiable adult and holds reliable identify. It could be establishing identity through a valid ID, but a simple check-the-box confirmation from P that he/ she is the parent (even though she has registered on the platform) is now unlikely to meet this standard.

Case 2:
C informs DF that she is a child and declares P as her parent. DF shall enable P to identify herself through its website, app or other appropriate means. **P identifies herself as the parent and informs DF that she herself is not a registered user on DF's platform.** Before processing C's personal data for the creation of her user account, DF shall, by reference to identity and age details issued by an entity entrusted by law or the Government with maintenance of the said details or to a virtual token mapped to the identity and age, check that P is an identifiable adult. P may voluntarily make such details available using the services of a Digital Locker service provider.

Takeaway from this case study: Permitting a child to open an account on a platform where the parent is not registered on the platform, may require checking identify and age details through government issued cards. Further, it is possible that **in such cases, parent may direct the platform to the digital locker. Again, access to digital locker shall have to be limited to the documentation required- may be one identify proof, as parent's privacy is also critical.**

Case 3:
P is opening an account for C and identifies herself as C's parent and informs DF that she is a registered user on DF's platform and has previously made available her identity and age details to DF. Before processing C's personal data for the creation of her user account, DF shall check to confirm that it holds reliable identity and age details of P and that P is an identifiable adult.

Takeaway from this case study: When the parent herself wants to open an account for the child while already holding an account for himself/herself, then rechecking would still be required. Suppose the identity proof submitted by the parent is lost, for some reason, then documents should be sought again.

Case 4:

P is opening an account for C and identifies herself as C's parent and informs DF that she herself is not a registered user on DF's platform. Before processing C's personal data for the creation of her user account, DF shall, by reference to identity and age details issued by an entity entrusted by law or the Government with maintenance of the said details or to a virtual token mapped to the identity and age, check that P is an identifiable adult. P may voluntarily make such details available using the services of a Digital Locker service provider.

Takeaway from this case study: This case study is similar to case study 2, except that the parent wants to open the account.

It is evident the DPDP Act and the DPDP Rules will require lot of submission of data by the parents and necessarily involve confirmations. It is left to the DF to identify what they consider reliable and necessary to demonstrate compliance.

However, the main question remains that if an individual submits a false age to sign on the platform i.e. a minor declares her date of birth incorrectly and gets access to the platform, who shall be held responsible?

- **WHAT ARE THE EXCEPTIONS WITH RESPECT TO THE DATA FIDUCIARIES?**

It is important to understand that not all data fiduciaries are covered by these strict obligations. DPDP Rules have a detailed schedule – Schedule IV- which specifically excludes certain fiduciaries provided they are meeting the conditions listed therein. For example, healthcare (including allied healthcare) professionals are excluded when processing is restricted to providing healthcare services. Some other examples are given below:

Class of Data Fiduciary	Condition	Examples
An educational institution- "educational institution" shall mean and include an institution of learning that imparts education, including vocational education."	Processing is restricted to tracking and behavioural monitoring— (a) for the educational activities of such institution; or (b) in the interests of safety of children enrolled with such institution.	Examples of educational institution could definitely include schools, colleges but would edtech companies be covered through this exception?
An individual in whose care infants and children in a crèche or child day care centre are entrusted.	Processing is restricted to tracking and behavioural monitoring in the interests of safety of children entrusted in the care of such institution, crèche or centre.	Typically, day cares have CCTVs. If a creche uses pics of the kids for its own marketing, then that would definitely fall out of the exception.

- **WHAT ARE THE EXCEPTIONS WITH RESPECT TO THE PURPOSE OF DATA PROCESSING?**

Certain purposes are also excluded from data processing provided they meet the requisite conditions. Specifically, any law enforcement agency or a certificate granting agency is not required to go through this process when it is processing data for discharging its duties in the interest of the child. Other routine purposes are also excluded provided processing is limited to that purpose alone- like processing for opening an email account or determination of a real time location for child's safety are excluded from the obligations. Thus, a parent using an App to track the location of child for child's safety should be considered valid.

- **Can the purpose of consent change under the DPDP Act, especially with respect to children?**

- The short answer is no.

Purpose driven consent is the fulcrum of the DPDP Act, and it is important that all DFs stick specifically to the purpose for which the data is obtained, specifically for children, as is clear from Schedule IV mentioned above.
For example, consider an EdTech app used by a 10-year-old child. At the time of sign-up, a parent gives consent for the app to track the child's learning progress to personalise lessons. Over time, the AI system begins classifying the child as a "slow learner" based on response speed and test performance. This label is then used to assign simplified content, reduce difficulty levels, or trigger automated alerts and initiate discounted coupons of lower grades.

While this may appear helpful, the child is now being profiled and categorised by an algorithm in ways that could affect confidence, future learning opportunities, or even how others perceive the child. The parent may never have explicitly consented to such classification and may object to this algorithmic labelling.

WAY FORWARD:

All entities getting children's data should conduct thorough internal checking of the documentation and practices to ensure that verifiable consent and reliable identity proof is obtained. Entities should take necessary strong safeguards to protect children's data and prevent breaches. Appropriate technical and organisational measures must be in place to ensure that children's personal information is not exposed to unnecessary risks.

Further processing of data should be specifically limited to the purpose for which it is obtained. Sharing or using data for which the consent does not exist may result in huge penalties. Any breach of the Data Fiduciary's obligations relating to the processing of personal data may attract penalties of up to Rupees Two Hundred Crores.

Maria Montessori, the great educationist once said- Children are human beings to whom respect is due, superior to us by reason of their innocence and of the greater possibilities of their future. It's time we demonstrate our respect to the kids by according enough protection to their data.

For any feedback or response on this article, the authors can be reached on aarti.banerjee@ynzgroup.co.in and ruchika.dave@ynzgroup.co.in

Author: Aarti Banerjee

Aarti is a Partner - Corporate Legal Advisory:

Aarti is experienced in corporate legal matters having specialization in drafting, vetting and negotiation of agreements. By qualification she is an advocate and a solicitor.

Co-author: Ruchika Dave

Ruchika Dave is an Advocate with around 9 years of experience in the field of Arbitration and Litigation. At YNZ she is at a position of Manager- Litigation. By qualification she is Bachelor in Law (BLS/LLB) from Pravin Gandhi College of Law, Mumbai.