

“VERIFIABLY SAFE” PROCESSING OF CHILDREN’S PERSONAL DATA UNDER THE DPDPA 2023 : A CATALOG OF MEASURES

November 2023

“VERIFIABLY SAFE” PROCESSING OF CHILDREN’S PERSONAL DATA UNDER THE DPDPA 2023 : A Catalogue of Measures

AUTHORS

Future of Privacy Forum

Bailey Sanchez

Christina Michelakaki

The Dialogue

Kamesh Shekar

Vaishnavi Sharma

Kazim Rizvi

CONTRIBUTORS

Future of Privacy Forum

David Sallay

Dominic Paulger

Sakshi Shivhare

The Dialogue

Akriti Jayant

The Future of Privacy Forum (FPF) is a global non-profit organization that brings together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of data use, identify the risks, and develop appropriate protections. FPF has offices in Washington D.C., Brussels, Singapore, and Tel Aviv.

The Dialogue™ is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

For more information

<https://fpf.org/> <https://thedialogue.co>

Suggested Citation

Sanchez, B., Michelakaki, C., Shekar, K., Sharma, V., & Rizvi, K. (2023, November). "Verifiably safe" processing of children's personal data under the DPDPA 2023: A Catalogue of Measures. The Dialogue™ & The Future of Privacy Forum.

Catalogue No.

TD/PDG/PB/1123/03

Publication Date

November 27, 2023

Disclaimer

The facts and information in this report may be reproduced only after giving due attribution to the authors, The Future of Privacy Forum and The Dialogue™.

INTRODUCTION

The [Digital Personal Data Protection Act, 2023](#) (DPDPA) provides for enhanced protection for children in respect of the processing of their personal data. Section 9 of the DPDPA mandates that before any such processing occurs, the data fiduciary obtains “verifiable consent” from the parent or lawful guardian of the child.¹ The DPDPA also includes two prohibitions concerning the processing of personal data of children. First, data fiduciaries must not engage in processing such data that is “likely to cause any detrimental effect on the well-being of a child.” Second, data fiduciaries are prohibited from “tracking or behavioral monitoring of children or targeted advertising directed at children.”

However, if the processing of personal data of children is done “in a manner that is verifiably safe,” the government has the competence to lower the age above which data fiduciaries may be exempt from all or some of these obligations. In addition, the government has the competence to grant exemptions based on the class of data fiduciary (e.g., education), provided that they meet certain predetermined criteria.

Against this backdrop, The Future of Privacy Forum (FPF), in collaboration with The Dialogue, prepared a list of measures that may be “verifiably safe” based on DPDPA related to the protection of children, advised by industry-leading best practices and approaches accepted in key jurisdictions² with experience in implementing data protection legal obligations geared towards children. Not all of these measures may immediately apply to all industry stakeholders. For instance, enhanced transparency requirements may be more applicable to certain online service providers and application developers than to other data fiduciaries and in any case, must be grounded in the notice obligations under the DPDPA. In fact, most of the measures proposed in this brief specify obligations in the DPDPA that consider the enhanced protection of children and their best interests when their personal data are processed.

The DPDPA’s concept of “verifiably safe” processing of children’s personal data is unique to the DPDPA and not found in other data protection regimes. Since an essential condition of the measures proposed to protect children’s privacy is that they must be “verifiable,” it is crucial that the measures are spelled out, implemented in a traceable way, and documented by data fiduciaries.

The catalogue/brief of “verifiably safe” measures we propose, strictly focuses on privacy safeguards related to the processing of personal data of children, in line with the scope of the DPDPA. While there are various facets to protecting children in the digital world, like reducing exposure to harmful online content and other online safety measures, these are dealt with under the scope of the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and will be addressed also under the upcoming Digital India Act. Therefore, to enhance transparency and accountability of the data fiduciaries related to processing of children’s personal data, this brief discusses “verifiably safe” measures with a strict focus on privacy.

As used in this document, “children” refers to everyone under 18, in accordance with the DPDPA’s definition of “minors”. “All individuals between 0 and 17” represents a developmentally diverse group who may have different needs and engage online in different ways. There are instances where we refer


¹ Verifiable parental consent (VPC) is a legal concept rooted in the Children’s Online Privacy Protection Act (COPPA, 15 USC § 6501(9)) in the United States, which is defined as any reasonable effort, taking into consideration available technology, to ensure that a parent authorizes the collection, use, and disclosure of a child’s data. FPF conducted a multi-year, multi-stakeholder process to understand the risks and limitations of COPPA’s VPC model and technologies used to obtain VPC, which resulted in the publication of a Report and Infographic in June 2023, “The State of Play: Is Verifiable Parental Consent Fit For Purpose?”, available at <https://fpf.org/verifiable-parental-consent-the-state-of-play/>




² Our survey of jurisdictions included law and regulatory action from Japan, Singapore, South Korea, United States, UK, and EU.



to “older teens” or “very young children” to highlight where a particular consideration may apply more to one end of this spectrum than the other. However, we do not make a specific age recommendation, as jurisdictions vary greatly in the age of digital consent and there is no one right answer. Ultimately, in all cases it is important to look at this list of measures through the lens that older teens and very young children may require unique considerations, even when a measure may ultimately benefit both ends of the developmental spectrum defined in the DPDPA.



We encourage further conversation between government, industry, privacy experts, and representatives of children, parents, and lawful guardians to identify which practices and measures may suit specific industry players.




Table: Measures for “Verifiably Safe” Processing of Children’s Personal Data



	VERIFIABLY SAFE MEASURE	PROPOSED ACTIONABLE CRITERIA FOR THE VERIFIABLY SAFE MEASURE, AND FURTHER CONTEXT
1.	 <p>Ensure enhanced transparency and digital literacy for children.</p>	<ul style="list-style-type: none"> • Children can be provided information on the service they are using beyond what is required in Section 5 DPDPA, so that they not only understand what data will be collected, for what purpose and what rights they have in relation to it, but also how their data will be used, and how and to whom their data will be disclosed. • Children can be provided information on tools and optional features available to edit privacy and safety settings. • Information provided to children should be easily understandable and in a language they speak and understand. Considering the developmental stage and reading capabilities of children, information may be delivered through cartoons, graphics, video, and audio content, especially if made to be interactive or gamified. • Data fiduciaries can provide non-written communication options, like emojis or “emotes”, standardized symbols, etc. • Push notifications can advise children to discuss issues with parents or lawful guardians (trusted adults). Trusted adults can be provided with information that helps them act in the best interest of the child and support their task. • Children should be able to voice their questions with regard to transparency information they received directly to the respected data fiduciary via an easily accessible channel such as an instant chat, or a privacy dashboard.



2.	 <p>Ensure enhanced transparency and digital literacy for parents and lawful guardians of very young users.</p>	<ul style="list-style-type: none"> • For very young users, parents can be provided information on the service their child is using to understand what data will be collected, how their child’s data will be used, and how their child’s data will be disclosed. • Parents or lawful guardians of the child can be provided information on tools and optional features available to edit privacy and safety settings for their child. • Information provided to parents or lawful guardians should be easily understandable.
3.	 <p>Opt for informative push notifications and provide tools for children concerning privacy settings and reporting mechanisms.</p>	<ul style="list-style-type: none"> • Make available a clear and easily accessible mechanism for reporting privacy concerns or violations. The mechanism should be functional at all times and must ensure the grievance is redressed within the time stipulated under the DPDPA. • Push notifications can inform children that another option provides a greater level of privacy than the action they are about to choose. • Tools should correspond to the capabilities of younger children, as developmentally appropriate.
4.	 <p>Provide parents or lawful guardians with tools to view, and in some cases, set children’s privacy settings and exercise privacy rights.</p>	<ul style="list-style-type: none"> • Potential parents/lawful guardians tools for children could include: viewing reported or blocked accounts, restricting the types of data that may be shared, viewing messaging settings, and viewing friends and followers lists. • Parents or lawful guardians should be afforded a clear and easily accessible mechanism for reporting privacy concerns or violations. The mechanism should be functional at all times and ensure the grievance is redressed within the time notified by the government under the DPDPA. • Consider what types of parental tools are appropriate depending on the age of the child and the nature of the data fiduciary’s service. For older teens, a parent making adjustments or being able to view all settings may be less appropriate.


<p>5.</p>	 <p>Set account settings as “privacy friendly” by default.</p>	<ul style="list-style-type: none"> • For services that offer the option of a public or private account, children’s accounts can be set to private by default. • For services that offer the option of connecting with accounts, children’s accounts can be, by default, set to not be “found” or “suggested,” only connecting if you have mutual friends, are the same age, attend the same school, etc., or to the most private option that is appropriate for the nature of the data fiduciary’s service. • If the service includes sharing content and data, the audience selections can be limited by default. • Privacy settings can be specific to the user rather than to the device. • By default, data fiduciaries can opt not to collect information about a child’s precise location or movements, unless necessary, including information inferred from a device’s GPS, Wi-Fi, Bluetooth, or other sensors. • Data fiduciaries should consider at what age it is appropriate to create an account on their service. • Consider whether the parent or the child should have the ability to change settings on sharing content and data. Also, consider whether very young users should be “locked” from changing certain settings.
<p>6.</p>	 <p>Limit advertising to children.</p>	<ul style="list-style-type: none"> • While the DPDPA prohibits targeted advertising directed at children, contextual advertising, or advertising based on the content of the page, is still possible and may be appropriate. Note that some data fiduciaries may rely on advertising to offer their product or service for free. • Data fiduciaries could consider placing notices on websites when a young user is leaving a site or service that is configured to limit advertising content or data collection and moving on to a site or service without such protections. • Data fiduciaries can provide notice and consent for combining behavioral information which may involve aggregating personal data for contextual advertising. • Ad trackers can be configured to prevent data collection from users under a specific age. • Consider whether older teens have the developmental capacity and maturity to

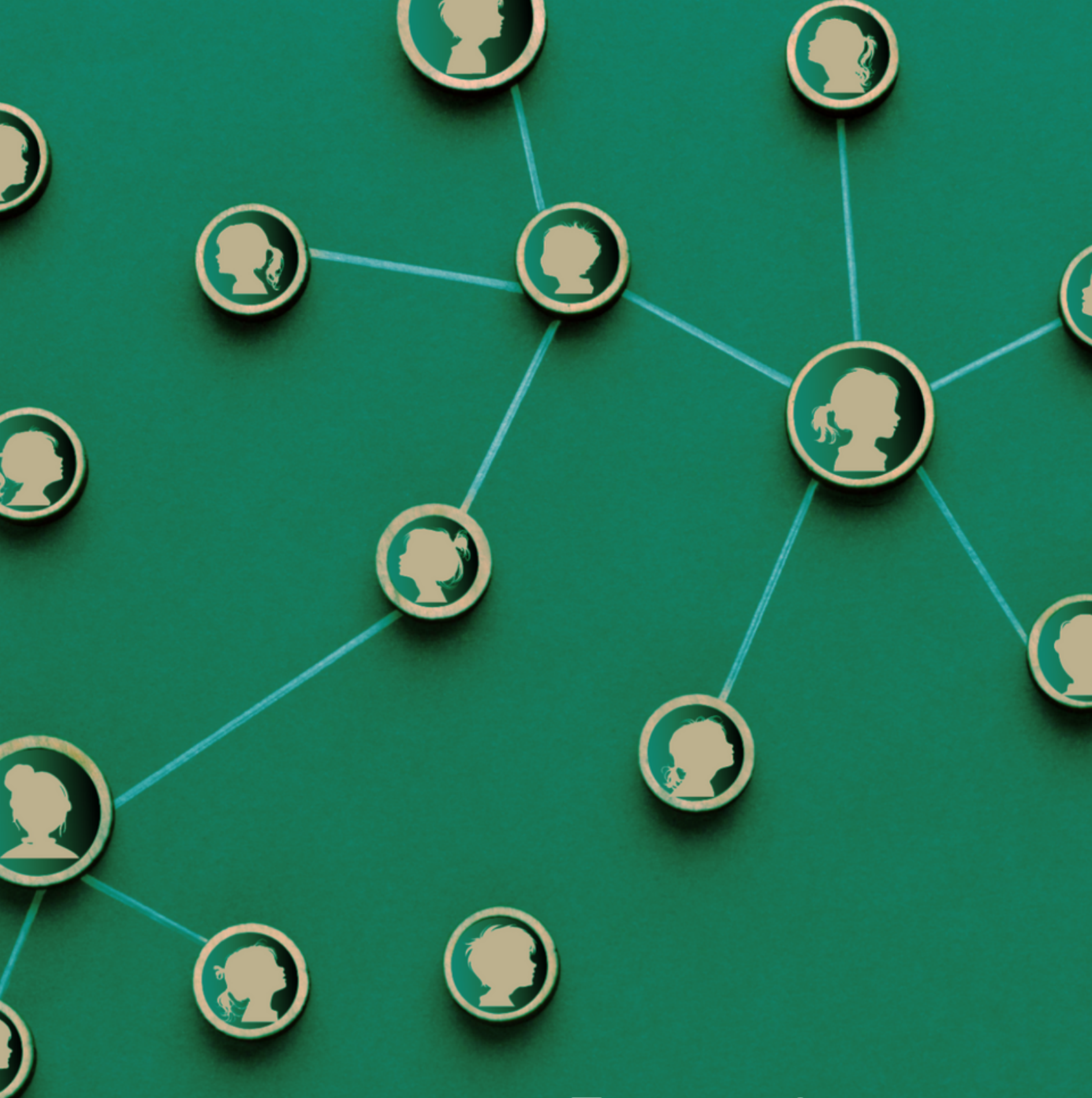
		make choices regarding their data processing.
7.	 <p>Maintain the functionality of a service at all times, considering the best interests of children.</p>	<ul style="list-style-type: none"> Consider whether some data processing may be necessary to maintain the function of the service, and/or whether this processing is in the best interests of children. Location information may be one such example.
8.	 <p>Adopt policies to limit the collection and sharing of children’s data.</p>	<ul style="list-style-type: none"> Data fiduciaries can restrict communicating and interacting with other users to a threshold age group. For social online experiences, communication and interaction can be set to friends only, family only, or only within the same age group. Voice communication can be retained for purposes of any possible content moderation, but consider which parties have access to this data and for how long. Data fiduciaries should establish concrete limits to data collection and sharing taking into account the user's age. As teens can demonstrate more readiness for online engagement than younger children, consider in which cases a prescriptive approach is more appropriate. If the data fiduciary opts to collect location movement, they should determine what level of precision is necessary to provide the service, if there is a reason to collect it by default that is also in the best interests of the child, and whether precision can be reduced.

9.	 <p>Consider all risks of processing their personal data for children and their best interests via thorough assessments.</p>	<ul style="list-style-type: none"> • Significant data fiduciaries must conduct data protection impact assessments under the DPDPA. Consider whether all data fiduciaries handling children’s data should conduct data protection impact assessments as a “verifiably safe” measure on a voluntary basis. • Data protection impact assessments can help evaluate and mitigate potential privacy risks associated with processing children’s data. • Consider whether data protection impact assessments should be audited, retained, reviewed, or require any mitigation plan. • Consider whether data protection impact assessments should evaluate the likelihood of children accessing a service that does not provide privacy protections for children.
10.	 <p>Ensure the accuracy of the personal data of children held.</p>	<ul style="list-style-type: none"> • Data fiduciaries can take proactive steps to ensure the accuracy of all personal data about a child being processed, especially where inaccuracy may have negative consequences for a child and her best interest. • Data fiduciaries should strike a balance between data accuracy and data collection by placing greater emphasis on the precision of data when it pertains to use cases having a significant impact on children. • Data accuracy efforts should be tailored to the unique characteristics of each data point taking into account the child's best interests and the mitigation of any potential harm.
11.	 <p>Use and retain personal data of children considering their best interests.</p>	<ul style="list-style-type: none"> • Children’s personal data should be processed according to their best interests, as defined under the UN Convention on the Rights of the Child, and avoid any detrimental use. • In line with the general obligations of data fiduciaries under Sections 8(7) and 8(8), children’s personal data should be configured to be deleted after the purposes for which they were collected no longer apply. • New purposes for the use of retained data can be made clear and explained to the user, who should be offered the chance to reset security and contact details.

		<ul style="list-style-type: none"> When a child becomes an adult or reaches a new age of consent, consider whether the data held while they were a child should be migrated to a newly-created account. It is possible the user may wish to remove or archive all or part of the data, including in cases where adults can override their parents’ or lawful guardians’ consent given when they were children.
12.	 <p>Adopt policies regarding how children’s data may be safely shared.</p>	<ul style="list-style-type: none"> Children’s personal data should only be shared when necessary and only the minimum amount of data should be shared for the necessary purpose. The link between the objective aimed and the sharing of the information should be documented. Furthering the enhanced transparency recommendation above, data fiduciaries can provide additional notice to children and their parents when data is shared with third parties. For instance, this notice could include the purpose for sharing and the intended recipient.
13.	 <p>Give children options in an objective and neutral way, avoiding deceptive language or design.</p>	<ul style="list-style-type: none"> Interfaces should not influence children’s choices regarding their data by appealing to their emotions or by using visual stimuli. Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design. The language used, including its tone and style, should be appropriate. The location of certain buttons, the phraseology used, and the difference in color gradient are other indicative factors that could nudge the child to a certain decision, leading them subconsciously to decisions that violate privacy interests. Consider that very young children may be more susceptible to manipulation than older children.

<p>14.</p>	 <p>Put in place robust internal policies and procedures for processing personal data of children and prioritize staff training.</p>	<ul style="list-style-type: none"> • Staff training on the appropriate use of personal data of children, including on “verifiably safe” processing, and internal policies, can increase awareness among staff on the sensitivity of handling such personal data, and mitigate the risk of unauthorized data disclosure. • Internal policies can encourage a privacy-by-design approach according to which children’s interests and rights are being protected from the beginning of processing activity and throughout the lifecycle of the data processing. • When developing or deploying a product or service, comprehensive guidance should exist on how to use privacy tools, and staff should be required to confirm that the issued guidance has been read and understood. Regular refresher sessions of training can be conducted.
<p>15.</p>	 <p>Enhance accountability for data breaches through notifying the parents or lawful guardians and adopting internal policies such as Voluntary Undertaking if a data breach occurs.</p>	<ul style="list-style-type: none"> • Further specifying the obligations under Section 8(6) of the DPDPA for personal data of children. If a data breach occurs, data fiduciaries can put policies in place so that the parents or legal representatives who are somehow engaged with the service that their child is using are notified promptly. • Consider whether it is appropriate to notify parents or lawful guardians in all instances or whether notification is appropriate for any data breach that results in, or that is likely to result in, significant harm to the child. • Consider whether and how the child should receive a breach notification, depending on their age and developmental level of understanding. • Further specifying the obligations under Section 32 of the DPDPA for the personal data of children, data fiduciaries could have policies in place to resolve grievances related to children’s personal data breaches with priority. • Consider taking first order action to remediate data breaches involving children’s personal data within the broader Voluntary Undertaking.

16.	 <p>Conduct specific due diligence with regard to children’s personal data when engaging processors</p>	<ul style="list-style-type: none">• Carefully evaluate and select processors to ensure they comply with data protection obligations for children.• Include specific clauses related to the protection of children’s personal data in the contracts between data fiduciaries and processors, pursuant to the obligation in Section 8(2) DPDPA. For instance, such clauses can obligate the processors to protect the personal data of children in accordance with the fiduciaries’ practices.• Evaluate whether processors adhere to robust DPDPA compliance programs before engaging them in a data processing activity.• Seek accreditations and certifications which may validate the children’s protection safeguards operationalized by data processors.
------------	--	---



The Dialogue™
INFORM ENGAGE IDEATE



thedialogue.co



[LinkedIn | The Dialogue™](#)



[Twitter | The Dialogue™](#)



[Facebook | The Dialogue™](#)



[Instagram | The Dialogue™](#)



**FUTURE OF
PRIVACY
FORUM**



fpf.org



[LinkedIn | Future of
Privacy Forum](#)



[Twitter | Future of
Privacy Forum](#)



[Facebook | Future of
Privacy Forum](#)



[Instagram | Future of
Privacy Forum](#)