ARTICLE NO. 5
PROTECTION OF CHILDREN'S PERSONAL DATA UNDER THE VIETNAMESE DRAFT LAW ON PERSONAL DATA PROTECTION AND THE GENERAL DATA PROTECTION REGULATION

Abstract: *This Article provides a comparative overview of Vietnam's Draft Law on Personal Data Protection ("**Draft Law**") and the EU General Data Protection Regulation ("**GDPR**"), focusing specifically on the protection of children's personal data. This article examines the key similarities and differences in how both legal frameworks define, regulate, and safeguard the data rights of children. The study aims to assess the extent to which the Draft Law aligns with international standards and identifies areas for potential legal development in Vietnam.*

Keywords: *#PersonalData #GDPRvsDraft Law #DataPrivacyLaw #GDPR #ChildrenPrivacy #DataProtection #ChildrenDataRights #ChildSafety*

I. Definition of children and processing of children's personal data under the Draft Law and the GDPR

The protection of children's personal data is a matter of special concern under both Vietnam's Draft Law on Personal Data Protection and the European Union's General Data Protection Regulation (GDPR). While both legal frameworks do not define "child" in a standalone manner, both set age thresholds for obtaining valid consent for processing children's data. However, these two legal frameworks take different approaches in setting the upper limit of children's age in order to establishing rules for the processing of children's personal data.

Age threshold of a "Child"

- Article 8(1) of the GDPR sets out an age threshold under 16, which requires the controller/processor to obtain consent of the parent or guardian of the children. However, GDPR allows Member States to provide for a lower age limit, provided it is not below 13. As such, under the GDPR, a "child" may be understood to refer to a person below the age of 16, 15, 14, or 13, depending on the Member State.

- Article 24 of the Draft Law sets out a requirement to obtain consent from both the child and their parent or guardian for the processing of personal data of individuals aged from 7 to under 15 years. This implies that the Draft Law treats individuals under 15 as children in the context of personal data protection.

While the Draft Law sets the threshold at under 15 years, it differs from Article 1 of the Law on Children 2016, which defines a child as anyone under 16. As a result, individuals aged 15 to under 16 may not be fully covered by specific child data protection safeguards under the Draft Law. This discrepancy may negatively affect these

individuals—legally children—who do not benefit from protections such as the dual consent requirement and the prioritization of their best interests. This inconsistency also creates legal uncertainty for data controllers, who may be unsure whether dual consent is needed for individuals aged 15 to under 16. Consequently, these children's personal data could be processed with a lower level of protection, undermining the law's intent.

II. Age of consent for processing children's personal data

The age of consent for processing children's personal data reflects each legal system's view on child autonomy, maturity, and the level of protection required in the digital environment.

The GDPR sets the default age of consent at 16 years but allows Member States to reduce this age to no lower than 13 years in accordance with Article 8 paragraph 1. As a result, the consent age varies across jurisdictions. For example, Ireland and Finland set the age at 13 (Section 5, Data Protection Act 1050/2018), while Spain sets it at 14 (Macenaite and Kosta (n 23), pp. 152–155), showing the flexibility permitted within the GDPR framework.

Under the Draft Law, individuals aged 7 to under 15 must provide consent along with their parent or guardian. However, those aged 15 to under 16 are not clearly covered, despite being classified as children under the Law on Children. This discrepancy introduces ambiguity into legal obligations and could leave a vulnerable group without adequate safeguards.

III. Verification Requirements for Processing Children's Personal Data

a) Challenges created by the Draft Law

According to the Draft Law, the processing of personal data of children aged from 7 to under 15 is only permitted with dual consent, meaning that both the child and their parent or legal guardian must give their approval. To ensure that this consent is lawful and valid, data controllers may be required to carry out an identity verification process as follows:

- ***Step 1:*** Verifying the age of the data subject: data controllers must determine whether the data subject falls within the 7 to under 15 age group, as this is the range that requires dual consent. This verification may require the user to provide a birth certificate, national ID card, passport, or other personal information to accurately confirm the child's age.

- ***Step 2:*** Verification of the parent or legal guardian's information: Once it has been confirmed that the data subject is a child, the data controller must proceed to collect

and verify information about the child's parent or legal guardian. This includes verifying the legal relationship between the child and the individual claiming the right to provide consent on their behalf, which may require documents such as a copy of the birth certificate, a court-issued guardianship decision, or other legal paperwork.

- ***Step 3:*** Verification of the marital or life/death status of the parent or guardian: To determine who holds the legal authority to give consent, the organization may also need to verify the marital status of the parents (e.g., whether they are divorced and who has custody) or whether the parent or guardian is deceased. This process could involve collecting sensitive personal data, such as genetic characteristics or other data classified as sensitive under personal data protection laws.

The verification process described above entails the creation and storage of a large volume of personal data, not only of the children but also of adults (such as parents or legal guardians). Collecting and processing such a substantial amount of data inevitably increases the risk of privacy breaches, especially given that Vietnam has yet to establish an effective personal data governance system or clear accountability mechanisms for data controllers. At the same time, this raises a critical question: Is a protective procedure unintentionally turning into an excessive surveillance and data collection mechanism, undermining the core principle of personal data protection?

b) In comparison with the GDPR

Most EU Member States have developed or are operating centralized and standardized population databases to support identity verification, including age and parental/guardian relationship verification. For example:

- Sweden: The Swedish Population Register maintains data on date of birth, personal ID number, parental relationships, marital status, and is integrated with public and private services.
- Finland: The Population Information System stores comprehensive individual and family relationship data, enabling accurate age and legal guardian verification.
- Germany: Maintains the Melderegister (mandatory residence registration system), which assigns a unique identifier and centralizes personal data.
- Estonia: A leading example of digital governance, where each citizen has a national ID code and can be securely verified through eID and platforms like X-Road.

Thanks to these standardized databases, privacy risks are reduced, as verification can be performed via temporary queries or API integrations without long-term storage of personal records. Organizations and authorities can reliably verify age, parental status, and custody rights without requiring manual submission of sensitive documents like birth certificates or family books.

However, GDPR restricts access to population data strictly to what is necessary, with clear purpose limitation and appropriate safeguards. As a result, private entities may not access population databases directly, instead using government-approved eIDAS services or certified third-party platforms.

IV. Circumstances for terminating, deleting, or destroying children's personal data

a) Lack of transparency and guidances under the Draft Law

Unless otherwise provided by law, the Draft Law requires data controllers to cease processing and delete or destroy children's personal data in the following situations:

(i) Personal data is being processed inconsistently with the original purpose, or the purpose has already been accomplished. For example, a summer camp that collects data for managing children's health and activities must delete the data after the camp ends.

(ii) Consent is withdrawn by the parent or legal guardian. For instance, if a parent revokes consent for their child's interview and photo in a magazine, the magazine must delete the content. But it should be noted that the withdrawal does not affect previously lawful processing.

(iii) Competent authorities determine that data processing harms the child's rights or interests. If, for example, an adult website collects a child's personal data without proper consent or age verification, competent authorities may require deletion of that data.

It can be concluded that the Draft Law only provides circumstances on terminating, deleting, or destroying children's personal data but lacks of transparency and specific guidances on how to obtain children's consent or implement appropriate safeguards when doing so. This creates a gap in ensuring the protection of children's rights throughout the data processing lifecycle. For detailed guidance, please refer to the GDPR for more useful insights when improving the legal framework of Vietnam in this area.

b) In comparison with the GDPR

The GDPR recognizes and gives children the same data rights as adults, while requiring additional conditions to be met due to children's vulnerability in the digital environment :

(i) **Transparency**: Article 12 and Recital 58 of the GDPR require that information (language) provided to children be clear and understandable. Depending on the child's age and cognitive ability, it's more effective to use images, videos, icons,

or gamified elements rather than plain text to convey information. If text is used, it should be visually engaging - broken into small sections, with bright colors, large fonts, and bullet points to make it easier to understand.

Organizations are not strictly required to provide separate transparency information for adults and children; as long as the content is clear enough for a child to understand, it can meet GDPR requirements. However, if the target audience includes children of varying ages, organizations should consider age-specific approaches or ensure that the way and timing of delivering the information make it accessible and understandable for children.

(ii) **Right to Erasure**: Article 17 and Recital 65 of the GDPR give children the right to delete personal data, especially data shared without fully understanding the risks.

Children often don't fully understand how their data is tracked, analyzed, and used. While they may know that an app is collecting data, concepts like *profiling*, *cross-device identification*, or *metadata* are much harder to grasp. They're also generally unaware that many "free" platforms operate by exchanging access for large amounts of personal data, including location, time of access, and online behavior. Therefore, when children or their parents or guardians wish to have their data deleted, a formal request must be sent to the data controller responsible for processing the data.

(iii) **Marketing**: Recital 47 of the GDPR allows data processing for marketing purposes based on legitimate interests. However, when it comes to children's data, those interests must not override or negatively impact the best interests of the child.

Obtaining a child's consent to process personal data for marketing must fully comply with the GDPR's requirements, meaning the consent must be freely given, specific, informed, and unambiguous (Articles 4(11) and 7 GDPR). Children must be able to understand the implications of agreeing to receive marketing content.

The Data Protection Commission (DPC) has stated that data processing for commercial purposes, including marketing, advertising, or behavioral profiling, generally fails to meet the principle of acting in the best interests of the child. However, there is no specific or fixed standard for determining the "best interests" of the child; this assessment is left to the data controller on a case-by-case basis. Therefore, unless an organization can clearly demonstrate that a specific marketing activity genuinely serves the child's well-being (e.g., promoting access to counseling services, educational, healthcare or social programs, or the work of child advocacy organizations), such processing should be avoided, with

consideration given to the actual context and processing practices of the data controller.

(iv) **Profiling and Automated Decisions**: Article 22 and Recital 71 advises against subjecting children to profiling or automated decision-making.

Profiling is a way of using someone's personal data to predict or analyze characteristics of that person, such as services they will be interested in, their likes or dislikes, preferences, views or opinions, or their behavior. For example, organizations may collect information about their customers or users to try to predict other services or products they might be interested in.

Profiling can also extend to using the personal data compiled in a profile on an individual to make automated decisions about them (e.g. using algorithms or artificial intelligence where there is no human element involved). Importantly Recital 71 of the GDPR says that measures relating to "*solely automated decision-making, including profiling, with legal or similarly significant effects*", "*should not concern a child*".

Profiling and automated decision-making can undermine the best interests of the child because they often operate without transparency, limit human oversight, and may lead to unfair, biased, or harmful outcomes that children are unable to understand or contest. Children are particularly vulnerable to being shaped or influenced by predictive models, especially in areas like targeted advertising, access to educational resources, or online content curation. When decisions are made solely by algorithms, without human intervention, they may fail to consider the nuanced and evolving needs of children, and could reinforce harmful stereotypes or exclude them from opportunities.

(v) **Access to Online Services**: Recital 38 of the GDPR provides an important exception to the general rule that parental consent is required to process children's personal data. Specifically, when online preventive or counselling services are offered directly to a child, the consent of a parent or legal guardian is not required. This exception ensures that children are not discouraged from seeking vital support, particularly in sensitive or urgent situations. However, this exemption applies only to services that are clearly designed for and targeted at children. Whether a service qualifies as such may depend on the assessment of competent authorities.

In certain situations, children may require counseling or support but may be unwilling or unable to communicate with their parents, for instance, in cases involving abuse, mental health issues, or psychological distress. This principle is that the requirement for parental consent must not act as a barrier to a child's

access to services that serve their best interests. This approach ensures the child's right to timely support is upheld, especially in cases where seeking parental involvement could deter them from accessing necessary help.

V. Challenges for further amendments of the Draft Law

a) Defining the age threshold for valid child consent in data processing

To enhance the Draft Law on Personal Data Protection, it is essential to revise the current age threshold for requiring dual consent to ensure consistency with existing Vietnamese laws. The current exclusion of individuals aged 15 to under 16 from the definition of "child" creates a legal gap, leaving this group without the full protections intended for minors. This ambiguity may lead to inconsistent application of the law and insufficient safeguards for a vulnerable age group that remains legally recognized as children.

b) Establishing reliable verification systems

Vietnam lacks a comprehensive, secure national data infrastructure for age and identity verification. This creates challenges for enterprises that must collect sensitive documents to comply with the Draft Law. There is a pressing need for a standardized, privacy-preserving digital identity system that can reliably confirm age and parent/guardian relationships.

Although Vietnam has promulgated a Law on Identification and various government decrees to empower the Ministry of Public Security in providing verification services and connection services to the National Population Database, it is to be seen how the Draft Law and private entities will benefit from the above-mentioned regulations in terms of processing children's personal data.

c) Ensuring child-appropriate consent and transparency in data processing

The absence of specific guidance on how to properly process children's personal data or obtain their valid consent presents substantial risks. Without clear standards, data processor may use complex or age-inappropriate language, making it difficult for children to understand what they are agreeing to. In some cases, systems might even include pre-ticked consent boxes, leading to passive or uninformed consent that does not meet the threshold for voluntary and informed agreement.

To address these concerns, the Draft Law should follow the GDPR and explicitly require the use of child-friendly consent mechanisms, set out clear principles for presenting personal data processing notices in a visual, age-appropriate, and easily understandable format. These notices should use plain language, icons, animations, or interactive

design elements to help children grasp what data is being collected, why it is needed, and how it will be used.

VI. Conclusion

The Draft Law's approach to children's data protection remains underdeveloped compared to the GDPR. It lacks coherence with domestic legal definitions, clear verification mechanisms, and detailed procedures for consent. Bridging these gaps requires legal reform, institutional capacity building, standardized identity infrastructure, and sector-specific guidance to ensure that children's rights are truly protected in the digital age.

AUTHOR(S)

TRAN DAI PHONG
Associate
E: phong.tran@asialegal.vn

NGUYEN THI MAI THU
Legal Assistant
E: thu.mai@asialegal.vn

CONTACT:

Telephone:
(+84) 24 2269 3399

Hotline:
(+84) 84 400 8484

Email:
info@asialegal.vn

Website:
https://dataprivacy.vn

Headquarter (Hanoi)
15th Floor, HT Building, No. 80 Duy Tan, Cau Giay District, Hanoi, Vietnam.

ABOUT ASIA LEGAL:

Asia Legal is one of the reputable business law firms in Vietnam. At Asia Legal, our commitment lies not only in providing conventional legal services but also in delivering tailored legal solutions that align with the business requirements of our clients. Our approach is founded upon an in-depth comprehension of Vietnamese legislation and a thorough understanding of the unique commercial landscape each client operates within.

To ensure the provision of high-quality service to our clients, we focus our endeavors exclusively on catering developing deeply to the service segments as follow:

- Mergers & Acquisitions
- Dispute Resolution
- Foreign Investment
- International Trade
- Energy & Natural Resources
- Real Estate & Construction
- Labor & Employment
- Data Privacy
- Intellectual Property

SCAN QR CODE TO JOIN US