

Research Article

PROTECTION OF CHILDREN'S PRIVACY AND PERSONAL DATA: A PERSPECTIVE FROM VIETNAMESE LAW

Thi Tuyet Dung Thai, Van Duong Nguyen* and Van Lam Nguyen

DOI:

<https://doi.org/10.33327/AJEE-18-9.3-a0002000>

Date of submission: 25 Apr 2026

Date of acceptance: 23 Jun 2026

Online First Publication: 23 Jul 2026

Last Publication: 05 Aug 2026

Disclaimer:

The views and opinions expressed in this manuscript are solely those of the authors and do not represent the views, policies, or positions of any affiliated institutions, organisations, or funding bodies.

Copyright:

© 2026 Thi Tuyet Dung Thai,
Van Duong Nguyen and Van Lam Nguyen

ABSTRACT

Background: *The protection of children's personal data is becoming an urgent issue in Vietnam and globally. This article analyses Vietnam's legal framework for the protection of children's personal data and addresses the specific legal question of how far Vietnam can adopt the legal elements currently set out in the General Data Protection Regulation (GDPR). It identifies structural limitations concerning age thresholds, consent mechanisms, sanctions, and the personal data protection authority. Finally, the article proposes recommendations and policy suggestions for improving the Vietnamese data protection law, including a developmentally stratified age-of-consent model and a specialised supervisory authority, with the broader aim of ensuring a safe digital environment oriented towards children's development.*

Method: *This article adopts a multi-method qualitative legal research design integrating three approaches: 1) a doctrinal legal analysis to identify, interpret, and evaluate Vietnam's normative framework; 2i) a functional comparative analysis is employed to compare Vietnamese law with the GDPR, to evaluate their degree of compatibility and to identify regulatory*

techniques that may be received into Vietnamese law; and 3) an interdisciplinary contextual analysis drawing on developmental psychology, cross-cultural psychology, and legal anthropology to evaluate children's decision-making capacity, family authority structures, and the influence of Confucian ethics, and 'Lang' culture on parent-child relationships, insights essential for adapting international models to Vietnam. Secondary sources, including peer-reviewed scholarship and international organisation reports, contextualise the findings.

Results and Conclusions: Although Vietnam has established a foundational framework, significant shortcomings persist: 1) the definition of "child" and age-based consent thresholds are inconsistent and insufficiently calibrated to children's evolving capacities; 2) the dual consent and suspension mechanisms lack clarity and sit uneasily with the cultural pressures that asymmetrically weaken a child's consent relative to a child's objection; 3) the sanctioning regime lacks adequate deterrent effect, notwithstanding recent amendments; and 4) Vietnam does not so much lack a supervisory authority as an independent one, its oversight function currently residing within the security apparatus, while it has no child-specific transparency, data protection by design, or data protection impact assessment (DPIA) obligations. On this basis, the article advances a framework of culturally conditioned legal transfer, classifying each GDPR technique as portable as it stands, requiring structural adaptation, or needing indigenous design, and proposes: (a) a tiered consent model with a qualified right for the child to object in high-risk processing; (b) child-specific transparency, data protection by design, and mandatory DPIAs; (c) a graduated, revenue-sensitive sanctioning regime; (d) a specialised data protection authority with relative independence and cross-border enforcement competence; (e) age-appropriate transparency in consent; and (f) deepened international cooperation. These reforms respect Vietnam's constitutional order and socio-cultural context.

1 INTRODUCTION

A recent study estimates that approximately one in three internet users worldwide is under eighteen.¹ In Vietnam, 83% of children aged twelve to thirteen use the Internet, rising to 93% among those aged fourteen to fifteen. A survey by the Institute for Research on Management of Sustainable Development (MSD Vietnam) and Save the Children International indicates that children spend five to seven hours per day on social media, while only 36%, primarily those aged sixteen to seventeen, have received education on online safety.² As a particularly vulnerable group, children benefit from the educational and recreational opportunities of digital technologies but also face significant risks of personal

1 Ingrida Milkaite and Eva Lievens, 'Children's Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm' (2019) 10(1) European Journal of Law and Technology 1.

2 Tổ Trang Lâm, 'Protect Children's Rights from Cyberviolence under the Vietnamese Law' (2025) 8(3) International Journal of Innovative Research and Scientific Studies 2689, doi:10.53894/ijirss.v8i3.7070.

data misuse and privacy infringements. Recognising this, many jurisdictions have adopted stringent legal frameworks to safeguard children online.³

In Vietnam, children's personal data protection has received increasing regulatory attention. Key instruments, including the Law on Personal Data Protection 2025 (LPDP),⁴ the Law on Children 2016,⁵ the Law on Cybersecurity 2018,⁶ and the Law on the Press 2016,⁷ have established a foundational framework. The Law on Advertising 2012,⁸ Decree 72/2013/ND-CP on Management, Provision and Use of Internet Services and Online Information 2013,⁹ and the Law on Handling of Administrative Violations 2012¹⁰ also play complementary roles. Nevertheless, academic research on this issue in Vietnam remains limited, resulting in persistent regulatory gaps that must be addressed to keep pace with the rapidly evolving digital environment.¹¹

Notably, the draft Decree on administrative sanctions in the field of personal data protection, currently under consideration by the Vietnamese government, represents a significant step toward enhancing deterrence. It is expected to introduce stringent penalties for violations involving personal data, including children's data. A cleaner sanctioning regime will strengthen children's privacy protection and contribute to a more transparent legal environment for digital sector businesses.¹²

-
- 3 Kathryn C Montgomery and Jeff Chester, 'Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework' (2015) 1(4) *European Data Protection Law Review* 277, doi:10.21552/EDPL/2015/4/6.
 - 4 Law of Vietnam No 91/2025/QH15 'On Personal Data Protection' (adopted 26 June 2025) <<https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Luat-Bao-ve-du-lieu-ca-nhan-2025-so-91-2025-QH15-625628.aspx>> accessed 17 April 2026.
 - 5 Law of Vietnam No 102/2016/QH13 'On Children' (adopted 05 April 2016) <<https://thuvienphapluat.vn/van-ban/Giao-duc/Luat-tre-em-2016-303313.aspx>> accessed 17 April 2026.
 - 6 Law of Vietnam No 24/2018/QH14 'On Cybersecurity' (adopted 12 June 2018) <<https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx>> accessed 17 April 2026.
 - 7 Law of Vietnam No 103/2016/QH13 'On the Press' (adopted 05 April 2016) <<https://thuvienphapluat.vn/van-ban/Van-hoa-Xa-hoi/Luat-Bao-chi-2016-280645.aspx>> accessed 17 April 2026.
 - 8 Law of Vietnam No 16/2012/QH13 'On Advertising' (adopted 21 June 2012) <<https://thuvienphapluat.vn/van-ban/Thuong-mai/Luat-Quang-cao-2012-142541.aspx>> accessed 17 April 2026.
 - 9 Decree of Vietnam No 72/2013/ND-CP 'On the Management, Provision and Use of Internet Services and Online Information' (adopted 15 July 2013) <<https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-72-2013-ND-CP-quan-ly-cung-cap-su-dung-dich-vu-Internet-va-thong-tin-tren-mang-201110.aspx>> accessed 17 April 2026.
 - 10 Law of Vietnam No 15/2012/QH13 'On Handling of Administrative Violations' (adopted 20 June 2012) <<https://thuvienphapluat.vn/van-ban/Vi-pham-hanh-chinh/Luat-xu-ly-vi-pham-hanh-chinh-2012-142766.aspx>> accessed 17 April 2026.
 - 11 Milkaite and Lievens (n 1) 1.
 - 12 'Draft Decree on Administrative Sanctions in the Field of Cybersecurity and Personal Data Protection' (*Ministry of Public Security of Vietnam*, March 2026) <<https://bocongan.gov.vn/chinh-sach-phap-luat/lay-y-kien-du-thao/ho-so-du-thao-nghi-dinh-quy-dinh-xu-phat-vi-pham-hanh-chinh-trong-linh-vuc-an-ninh-mang-va-bao-ve-du-lieu-ca-nhan-1772531021?type=dang-lay-y-kien>> accessed 16 June 2026.

The central question this article pursues is not whether Vietnam should follow the GDPR, but how far it can. Vietnam's Law on Personal Data Protection 2025 already mirrors much of the European model, yet a borrowed rule does not always behave the same way once it enters a different legal and cultural setting. A child's right to consent, for instance, presupposes a child who can speak independently of their parents, an assumption that sits uneasily with the Confucian and communitarian fabric of Vietnamese family life. The analysis, therefore, proceeds along two lines of inquiry. The first asks where the Vietnamese framework falls short when compared with how the GDPR addresses the same problems. The second asks which of those European solutions Vietnam can realistically borrow, which it must reshape, and which it cannot adopt without a domestic alternative. Read together, these questions treat each part of the Vietnamese framework as an instance of conditioned transfer, in which some techniques can be taken as they stand, others require structural adaptation, and a few must be rebuilt to fit Vietnamese conditions. The age threshold, the consent architecture, the sanctioning regime, and the supervisory authority are examined not as separate problems but as four points at which this same tension between the imported rule and the receiving context must be resolved.

2 METHODOLOGY

The article employs a multi-method qualitative legal research design integrating doctrinal legal analysis, comparative law, and interdisciplinary contextual analysis. This combination is essential, as the research questions concern not only normative content but also the socio-cultural conditions that govern the law's interpretation and enforcement, an issue that neither a purely doctrinal nor a purely sociological approach can fully address.

First, the doctrinal legal analysis method is utilised to systematically identify, interpret, and evaluate the legal system governing the protection of children's personal data in Vietnam, clarifying its normative substance, internal consistency, and existing legal gaps.

Second, the functional comparative law method compares the Vietnamese framework with the GDPR. The GDPR is chosen not merely for its regulatory maturity but because it is the very model the LPDP 2025 emulates, so the comparison reflects a transfer rather than an arbitrary pairing of two systems. The comparison is conducted across the following aspects: (i) GDPR instruments and provisions, including Recital 38, Articles 6, 7, 8, 12, 25, 35, 51–59 and 83 of the GDPR, the European Data Protection Board's (EDPB) guidelines 03/2022 on dark patterns and guidelines 02/2023 on Article 8; (ii) evaluative criteria, including the conceptualisation of children as data subjects and the applicable age thresholds, the structure of parental consent and children's evolving capacities, child-oriented transparency obligations and privacy-by-design requirements, revenue-based sanctioning mechanisms, and the design of supervisory authorities; and (iii) the functional comparative element, which asks how each legal framework addresses the same regulatory problem, namely the protection of children's data in the digital environment. The secondary sources are confined

to peer-reviewed scholarship; instruments of standard-setting bodies such as the EDPB, the UN Committee on the Rights of the Child, and the Organisation for Economic Co-operation and Development (OECD); and official enforcement decisions, so that the normative claims rest on authoritative rather than incidental materials. On this basis, the reform proposals are reached through a four-step process. The article first identifies the regulatory problem common to both systems, then maps how each system addresses it, then tests each GDPR technique against Vietnam's constitutional, institutional, and socio-cultural conditions, and finally classifies the outcome as a technique that is portable as it stands, one that requires structural adaptation, or one that must be designed indigenously. The recommendations in Section 4 follow directly from this classification.

Third, interdisciplinary contextual analysis integrates insights from three fields: (i) developmental psychology, to evaluate children's decision-making capacity at various consent thresholds; (ii) cross-cultural psychology, to analyse authority structures within the Vietnamese family; and (iii) legal anthropology, to elucidate the influence of Confucian ethics and "Lang" culture on parent-child relationships. These insights supplement rather than replace the legal analysis, providing a basis for adapting Western legal references to the Vietnamese context.

3 RESULTS AND DISCUSSION

3.1. Children, Children's Personal Data, and Children's Personal Data Protection

Under Vietnamese law, a "child" is defined as a person under the age of 16.¹³ This definition, as provided in the Law on Children 2016, differs from that set out in the United Nations Convention on the Rights of the Child (UNCRC), to which Vietnam acceded in 1990 and which all Member States of the European Union have ratified. The Convention provides that "a child means every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier."¹⁴ The GDPR does not adopt a uniform definition of "child" but anchors child-specific protection in Article 8, which sets the default age of digital consent at sixteen while permitting Member States to lower it to no less than thirteen. This margin has produced a heterogeneous European landscape (thresholds ranging from thirteen to sixteen), operating against the common backdrop of the UNCRC's 18-year benchmark. The definition of "child" thus varies across jurisdictions, reflecting differing cultural, legal, social, and historical contexts that shape how states conceptualise and protect children's rights.¹⁵ The Civil Code 2015 provides that

13 Law of Vietnam No 102/2016/QH13 (n 5) art 1.

14 Convention on the Rights of the Child (adopted 20 November 1989 UNGA Res 44/25) [1999] UNTS 1577/3, art 1.

15 Sonia Livingstone and others, 'Children's Rights and Online Age Assurance Systems: The Way Forward' (2024) 32 International Journal of Children's Rights 721, doi:10.1163/15718182-32030001.

a person attains full legal capacity at eighteen.¹⁶ Individuals aged sixteen to under eighteen, therefore, occupy an ambiguous legal position. They fall outside the scope of the Law on Children 2016 and have not attained the full legal capacity of adults under the Civil Code 2015. This lacuna is problematic because individuals in this age bracket have not yet achieved full physical, mental, and cognitive maturity and thus remain particularly vulnerable in the digital environment.

Pursuant to the LPDP,¹⁷ personal data is defined as information in symbolic, alphabetic, numeric, image, sound or similar electronic form that is associated with or capable of identifying a specific individual, encompassing basic and sensitive personal data. Neither this law nor other instruments define “children’s personal data”. Accordingly, the concept must be derived from the definition of “child” in the Law on Children 2016, read in conjunction with the general definition of personal data, which differs only in terms of the subject’s age.¹⁸

Empirical evidence underscores the urgency of strengthening children’s data protection in Vietnam. A 2020 survey conducted by MSD and Save the Children International (SCI) across seven provinces and cities found 96.9% of surveyed children had access to internet-connected devices.¹⁹ Children are also exposed to wide-ranging online risks; MSD reports that 40% felt unsafe online and over 70% had experienced negative incidents, including disclosure of personal information, harassment, and cyberbullying²⁰. The National Centre for Missing and Exploited Children reported over 700,000 child sexual abuse images originating from Vietnam, among the highest in Southeast Asia, after the Philippines and Indonesia.²¹ Vietnam ranked 28th of thirty economies in the DQ Institute’s 2020 Child Online Safety Index (12.7/100 compared to a global average of forty-two), with particularly poor performance on cyber risk and social infrastructure (the legal and policy framework for online child protection). The United Nations Children’s Fund (UNICEF) reports that

16 Law of Vietnam No 91/2015/QH13 ‘Civil Code’ (adopted 24 November 2015) art 20 <<https://thuvienphapluat.vn/van-ban/EN/Quyen-dan-su/Law-No-91-2015-QH13-The-Civil-Code/303230/tieng-anh.aspx>> accessed 17 April 2026.

17 Law of Vietnam No 91/2025/QH15 (n 4) art 2(1).

18 Milda Macenaite and Eleni Kosta, ‘Consent for Processing Children’s Personal Data in the EU: Following in US Footsteps?’ (2017) 26(2) Information & Communications Technology Law 146, doi:10.1080/13600834.2017.1321096.

19 Management and Sustainable Development Institute, *Voice of Vietnamese Children: Report on Survey Results* (MSD Vietnam 2020) 31 [in Vietnamese].

20 ‘Children Face Risks in Cyberspace with 87% Accessing Internet Daily’ (*VietnamPlus*, 19 March 2023) <<https://en.vietnamplus.vn/children-face-risks-in-cyberspace-with-87-accessing-internet-daily-post250092.vnp>> accessed 29 January 2026.

21 NCMEC, ‘2021 CyberTipline Reports by Country’ (*National Center for Missing & Exploited Children*, 2022) <<https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-country.pdf>> accessed 30 January 2026.

cyberbullying in Vietnam commonly occurs on Facebook, messaging applications (Zalo, Viber, etc.) and content-sharing platforms (YouTube and Instagram).²²

These data show that although Vietnam ranks among countries with high levels of internet and social media uptake among children, online safety, particularly regarding personal data, remains a significant concern. Comprehensive protection mechanisms are therefore needed for the following reasons:

First, children constitute a particularly vulnerable group. They are increasingly used for analytics, profiling, targeted advertising, and automated decision-making, while children often lack the capacity to comprehend the long-term consequences of such processing.²³ This renders them especially susceptible to identity theft, online harassment, and exploitation. UNICEF has emphasised that children's attitudes, preferences, and identities are continuously evolving and that their limited capacity for informed decision-making poses distinct privacy challenges. Even where children consent to data collection, they are generally unable to fully assess its long-term implications for their privacy.²⁴ In 2024, 1.1 million cases of child identity theft were recorded, with 50% of victims aged six or younger.²⁵ Children therefore require enhanced protection due to their incomplete physical and psychological development²⁶ and their classification as a vulnerable group with limited access to effective remedies.²⁷ Although these risks apply to all users, the harm is amplified when such technologies are deployed against children, who cannot give genuinely informed consent.²⁸

Second, children's personal data protection is intrinsically linked to their right to privacy in the digital environment. Article 16 of the UNCRC provides that no child shall be subjected to arbitrary or unlawful interference with privacy, family, home, or correspondence, or to unlawful attacks on honour and reputation, and the child has the right to legal protection against such interference or attacks. This right is reinforced by Article 8 of the European

22 Quy Nguyen, 'Vietnam Fares Poorly in Online Child Safety Ranking' *VnExpress International* (Hanoi, 15 February 2020) <<https://e.vnexpress.net/news/vietnam-fares-poorly-in-online-child-safety-ranking-4053720.html>> accessed 1 February 2026.

23 Sara M Grimes, 'Responsible AI and Children: Towards a Rights-Based Approach to AI Governance' (Sesame Workshop, Joan Ganz Cooney Center, 23 January 2025) <<https://joanganzcooneycenter.org/2025/01/23/responsible-ai-and-children/>> accessed 3 February 2026.

24 Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, *Children's Data and Privacy Online: Growing Up in a Digital Age* (LSE Media and Communications 2019) 15, 20, 25; Carly Nyst, Patrick Geary and Amaya Gorostiaga, *Privacy, Protection of Personal Information and Reputation Rights* (Discussion Paper Series: Children's Rights and Business in a Digital World, UNICEF 2017).

25 Julija A, 'Most Worrying Identity Theft Statistics for 2026' (*Fortunly*, 27 March 2026) <<https://fortunly.com/statistics/identity-theft-statistics/>> accessed 7 February 2026.

26 Mariya Stoilova, Rishita Nandagiri and Sonia Livingstone, 'Children's Understanding of Personal Data and Privacy Online: A Systematic Evidence Mapping' (2021) 24(4) *Information, Communication & Society* 557, doi:10.1080/1369118X.2019.1657164.

27 Darina Smyr and Ekaterina Ulianova, 'Legal Issues of Children's Personal Data Protection' (2022) 5(1) *Open Journal for Legal Studies* 1, doi:10.32591/coas.ojls.0501.01001s.

28 Milkaite and Lievens (n 1).

Convention on Human Rights (ECHR) and Article 12 of the UDHR.²⁹ In the digital environment, the right to privacy is inextricably linked to personal data protection. Any discussion of children's personal data necessarily engages their right to privacy.³⁰ Recital 38 GDPR acknowledges that children merit specific protection regarding their personal data, as they may be less aware of the risks, consequences, safeguards, and their rights. The GDPR's child-specific provisions reflect a broader commitment to aligning data protection with the best interests of the child.³¹ Although closely related, the two rights are not identical: privacy rights prohibit state interference in the personal sphere and in the formation of identity, whereas data protection establishes a control system over how personal information is processed by public and private entities.³² Children are particularly susceptible to privacy violations because of many situations in which adults exercise power over them. Any collection, processing, or sharing of their data constitutes a direct interference with privacy, which international and national law are obliged to protect.

Third, protecting children's data is essential to prevent misuse for unlawful purposes. Once disclosed within big data ecosystems, such data may be exploited for inappropriate advertising, behavioural manipulation, or criminal targeting. Children are no longer passive recipients of goods and services but increasingly act as consumers, contracting parties, and autonomous users.³³ However, limited awareness and digital literacy make them particularly susceptible to exploitation. Commercially, children are subject to large-scale profiling for behavioural advertising.³⁴ These practices feed children's data into algorithmic systems for

29 Council of Europe, *European Convention on Human Rights: as amended by Protocols Nos 11, 14 and 15; supplemented by Protocols Nos 1, 4, 6, 7, 12, 13 and 16* (ECtHR 2013).

30 Ahmad Sofian and others, 'Children's Privacy and Data Protection in Judicial Decisions in Indonesia' (2021) 18(4) *US-China Law Review* 153, doi:10.17265/1548-6605/2021.04.001.

31 Eva Lievens and Valerie Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34(2) *Computer Law & Security Review* 271-5, doi:10.1016/j.clsr.2017.09.007; Ingrida Milkaitė and Milda Mačėnaitė, 'Advancing Children's Privacy and Data Protection Rights: Emerging Data Protection Trends and Challenges in Selected CEE Countries' in Agnė Limantė and Rūta Vaičiūnienė (eds), *Children's Rights in Central and Eastern Europe: A Comparative Analysis with a Spotlight on Lithuania* (Springer 2025) 325, doi:10.1007/978-3-032-07092-0_16.

32 Sonia Livingstone and others, 'Children's Privacy in the Digital Age: US and UK Experiences and Policy Responses' in Dimitri A Christakis and Lauren Hale (eds), *Handbook of Children and Screens: Digital Media, Development, and Well-Being from Birth Through Adolescence* (Springer 2025) 491, doi:10.1007/978-3-031-69362-5_67.

33 Federica Persano, 'GDPR and Children Rights in EU Data Protection Law' (2020) (spec) *European Journal of Privacy Law & Technologies* 32.

34 Eline L Leijten and Simone van der Hof, 'Dissecting the Commercial Profiling of Children: A Proposed Taxonomy and Assessment of the GDPR, UCPD, DSA and AI Act in Light of the Precautionary Principle' (2025) 57 *Computer Law & Security Review* 106143, doi:10.2139/ssrn.5055046; Valerie Verdoodt and Eva Lievens, 'Targeting Children with Personalised Advertising: How to Reconcile the (Best) Interests of Children and Advertisers' in Gert Vermeulen and Eva Lievens (eds), *Data Protection and Privacy under Pressure: Transatlantic Tensions, EU Surveillance and Big Data* (Maklu 2017) 313.

profiling and personalised advertising; data are also traded across actors; for example, a website may sell a child's behavioural data through real-time bidding to the highest bidder, who then targets advertising at the children.³⁵ Children are more vulnerable to such advertising than adults, given their underdeveloped ability to recognise persuasive intent and limited awareness that social media data are being commercially exploited.³⁶ Additionally, digital platforms deploy dark patterns, deceptive interface designs that nudge users against their best interests, to which children are particularly susceptible.³⁷ The EDPB's 2023 Guidelines acknowledge dark patterns' especially harmful effects on children, who may be less aware of the risks and consequences associated with the processing of their personal data.³⁸ From a criminal perspective, according to Childlight (University of Edinburgh), more than 300 million children globally are victims of online sexual exploitation and abuse each year.³⁹ In 2024, the National Centre for Missing and Exploited Children (NCMEC) recorded 546,000 reports of online enticement, representing a 192% increase compared to 2023.⁴⁰ Children's data protection is therefore an urgent imperative against increasingly commercial exploitation and criminal abuse online.

Fourth, personal data protection is a fundamental condition for children's safe development online. The digital ecosystem presents both opportunities and risks. When appropriately safeguarded, children's online participation can help support their development. Privacy thus functions both as a protective right and an enabling right: shielding children from harm and providing the foundation for meaningful participation in digital life.⁴¹ Inadequate

-
- 35 Simone van der Hof and others, 'The Child's Right to Protection Against Economic Exploitation in the Digital World' (2020) 28 *The International Journal of Children's Rights* 833, doi:10.1163/15718182-28040003.
 - 36 Jenny Radesky and others, 'Digital Advertising to Children' (2020) 146(1) *Pediatrics* e20201681, doi:10.1542/peds.2020-1681; Esther Rozendaal and Moniek Buijzen, 'Children's Vulnerability to Advertising: An Overview of Four Decades of Research (1980s–2020s)' (2023) 42(1) *International Journal of Advertising* 78, doi:10.1080/02650487.2022.2135349.
 - 37 Jenny Radesky and others, 'Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children' (2022) 5(6) *JAMA Network Open* e2217641, doi:10.1001/jamanetworkopen.2022.17641; René Schäfer and others, 'Growing Up with Dark Patterns: How Children Perceive Malicious User Interface Designs' (NordCHI 24: 13th Nordic Conference on Human-Computer Interaction, Uppsala, Sweden, 13-16 October 2024) doi:10.1145/3679318.3685358.
 - 38 Arianna Rossi and others, 'Who Is Vulnerable to Deceptive Design Patterns? A Transdisciplinary Perspective on the Multi-Dimensional Nature of Digital Vulnerability' (2024) 55 *Computer Law & Security Review* 106031, doi:10.1016/j.clsr.2024.106031.
 - 39 Global Child Safety Institute, *Into the Light: Childlight Global Index of Child Sexual Exploitation and Abuse Prevalence* (Childlight 2024) <<https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-globa>> accessed 14 March 2026.
 - 40 WeProtect Global Alliance and Columbia University, *Global Threat Assessment 2025* (WeProtect 2025) <<https://www.weprotect.org/global-threat-assessment-25/>> accessed 14 March 2026.
 - 41 UN CRC, *General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment* (UN Doc CRC/C/GC/25, 2 March 2021) paras 67–76 <<https://digitallibrary.un.org/record/3906061>> accessed 14 March 2026; Stoilova, Nandagiri and Livingstone (n 26).

data protection exposes children to continuous monitoring and commercialisation; predefined algorithmic profiling can confine them to matched recommendations, depriving them of exposure to other content and hindering exploration and development.⁴² The protection of personal data is therefore a prerequisite for ensuring that children can benefit from the digital environment safely and comprehensively.

In sum, children's data protection is a critical policy and legal priority for Vietnam, both for children's safe development and for the broader human rights and privacy framework.

3.2. The current state of the legal framework on children's personal data protection in Vietnam

3.2.1. Recognition of children's personal data protection

The Vietnamese legal system on children's personal data covers multiple regulatory relationships. At the highest level, the Constitution 2013 provides the foundation for protecting privacy: everyone has the right to the inviolability of private life, personal and family secrets, and the right to the protection of honour and reputation.⁴³ The collection, storage, use, and disclosure of such information require the person's consent except as provided by law. This provision thus grounds individual privacy and serves as a foundation for more detailed provisions in other laws.

In addition to the Constitution, a series of laws and implementing documents address children's personal data and privacy. Among these, the Law on Children 2016 is a key instrument for protecting, caring for, and educating children. It sets out children's rights and the responsibilities of agencies, organisations, families, and individuals. Accordingly, Article 21 provides that children have the right to the inviolability of private life, personal and family secrets, and to legal protection of their honour, dignity, reputation, and the confidentiality of correspondence; the processing of children's personal data requires the consent of the child or lawful guardian.⁴⁴ The Government then issued Decree 56/2017/ND-CP ("Decree 56"),⁴⁵ detailing this law, the first Vietnamese instrument to define "private personal information relating to children" and set out protective measures online. Such information includes identifying characteristics; health records; images; family and caregiver data; residential

42 Hof and others (n 35) 835.

43 Constitution of the Socialist Republic of Vietnam (adopted 28 November 2013) art 21 <<https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Constitution-dated-November-28-2013-of-the-socialist-republic-of-Vietnam-221949.aspx>> accessed 14 March 2026.

44 Law of Vietnam No 102/2016/QH13 (n 5).

45 Decree of Vietnam No 56/2017/ND-CP 'Detailing a Number of Articles of the Law on Children' (adopted 9 May 2017) <<https://thuvienphapluat.vn/van-ban/Van-hoa-Xa-hoi/Nghi-dinh-56-2017-ND-CP-huong-dan-Luat-tre-em-340397.aspx>> accessed 14 March 2026.

address; and contact information, and information on school, academic performance, friends, and services used. Online disclosure of such information requires the consent of both parents and, where the child is seven or older, of the child as well.

Additionally, Article 54 establishes responsibilities for protecting children's private lives: agencies, organisations, educational institutions, families, and individuals must protect children's privacy and promptly notify the competent authorities upon detecting any infringements.⁴⁶ This creates a multi-actor, multi-layered network in which not only state authorities but also families, schools, and society bear responsibility, with the notification duty providing a rapid response mechanism. However, implementation remains constrained by uneven community awareness, particularly among families and schools, of the importance of protecting children's privacy.

Beyond the Law on Children, Decree 56 and the LPDP contain detailed provisions on children's personal data in Vietnam. Other instruments also apply. The Law on Cybersecurity 2018 grants children the right to be protected, to access information, to participate in social activities, to play, to maintain personal secrecy and privacy, and to enjoy other rights in cyberspace. Information system administrators and telecom, Internet, and value-added service providers must control information content so as not to harm or infringe upon children, prevent the sharing of, and remove, harmful content, and promptly notify and coordinate with specialised cybersecurity forces under the Ministry of Public Security for handling.⁴⁷ The Law's scope extends beyond personal data to harmful acts such as inducing children into unlawful activities. The Law on the Press 2016 protects personal secrets, including those of children, while the Law on Advertising 2012 prohibits advertising that uses an individual's images, words, or writings without consent. Policy measures reinforce this framework. Decision 830/QD-TTg approving the Programme on Protecting and supporting children to interact in a healthy and creative manner in the online environment for the period 2021–2025 and Decision 1591/QD-TTg approving the Programme on Child Mental Health Care and Care for Orphaned Children for the period 2023–2030 require the promotion of legal frameworks and cooperation with Internet service providers and technology enterprises.⁴⁸

46 Law of Vietnam No 102/2016/QH13 (n 5) art 54.

47 Law of Vietnam No 24/2018/QH14 (n 6) art 29.

48 Decision of the Prime Minister No 830/QD-TTg 'Approving the Program "Protecting and supporting children's healthy and creative interaction in the online environment during the period 2021–2025"' (adopted 1 June 2021) <<https://vanban.chinhphu.vn/default.aspx?pageid=27160&doid=203332>> accessed 16 March 2026; Decision of the Prime Minister No 1591/QD-TTg 'Approving the Program on Mental Health Care for Children and Care for Orphaned Children for the period 2023–2030' (adopted 8 December 2023) <<https://vanban.chinhphu.vn/?pageid=27160&doid=209145>> accessed 16 March 2026.

3.2.2. Children's right to consent to personal data protection

The LPDP builds its consent rule on a sliding scale of age. Under Article 24(2),⁴⁹ a child under seven has no voice at all, consent resting solely with the representative, while a child aged seven to under sixteen must consent jointly with the representative for the publication or disclosure of private matters. The structure already signals the tension this section examines, since it grants the child a formal say at precisely the age range where, in the Vietnamese context, that say is least likely to be freely exercised. This difficulty becomes clearer when the dual consent model is read against the backdrop of Vietnamese culture, shaped by Confucian philosophy and “Lang” culture.

The design of a dual consent mechanism for processing personal data under the LPDP does not necessarily increase substantive protection; it may instead create practical difficulties.

First, in terms of its ideological foundation, Confucianism places the parent-child relationship at the centre of the moral order, structured by the principle of hierarchy and the duty of filial piety. Filial piety is not only an emotion but also a normative obligation that requires children to respect, obey, and place family interests above their own will.⁵⁰ In a vertically structured authority where the parental will plays a guiding role, and in light of cross-cultural analyses of vertical collectivism in East Asian societies, acting against parental wishes is regarded not merely as a personal choice but as a deviation from moral norms.⁵¹ This is reinforced in the context of Vietnam’s “Lang” culture, whose basic social unit is the interwoven structure of “family-lineage-village,” where collective values stand above individual ones, and the family’s honour remains subject to the observation of the village community.⁵² The conduct of each member is tied to the face of the entire family and lineage, so the tendency to follow one’s parents derives not only from family authority but also from social pressure.

49 Law of Vietnam No 91/2025/QH15 (n 4) art 24(2).

50 Donghyun Kim, ‘The Concept of Filial Piety in East Asian Confucian Culture from the Perspectives of Gadamer and Habermas’ (2019) 33-34 *Kritika Kultura* 36.

51 Olwen Bedford and Kuang-Hui Yeh, ‘The History and the Future of the Psychology of Filial Piety: Chinese Norms to Contextualized Personality Construct’ (2019) 10 *Frontiers in Psychology* 100, doi:10.3389/fpsyg.2019.00100; Bart Soenens and others, ‘The Moderating Role of Vertical Collectivism in South-Korean Adolescents’ Perceptions of and Responses to Autonomy-Supportive and Controlling Parenting’ (2018) 9 *Frontiers in Psychology* 1080, doi:10.3389/fpsyg.2018.01080; Eunice Pui-Yu Yim, ‘Effects of Asian Cultural Values on Parenting Style and Young Children’s Perceived Competence: A Cross-Sectional Study’ (2022) 13 *Frontiers in Psychology* 905093, doi:10.3389/fpsyg.2022.905093.

52 Luong Ha Chuc Quynh, ‘The Influences of Collectivism on Vietnamese Communication Style’ (2021) 4(7) *International Journal of Research in Engineering, Science and Management* 10; Thi Kim Dung Le, ‘Characteristics of Traditional Vietnamese Family and Its Influence on Communication Culture in the Family’ (2021) 1(11) *Anthropological Researches and Studies* 49, doi:10.26758/11.1.4.

The system of village conventions, customary rules, and traditional patriarchal order further reinforces hierarchical family structures, with the principle that “Custom rules the law” reflecting the strength of community norms governing father–child, siblings, and spousal relationships.⁵³ Norms such as “Three Obediences and Four Virtues” and the preference for sons in traditional society have contributed to maintaining a patriarchal family model, in which the will of the head of the family is decisive.⁵⁴ Children are thus influenced both by their parents and by community opinion; the fear that “the whole village will know” functions as an effective mechanism of social control. Filial piety in Vietnam extends beyond the family to the honour of ancestors, lineage, and homeland so that obeying parents is internalised as a responsibility toward the community.

From the perspective of developmental psychology, children aged seven to eleven are in the concrete operational stage (Piaget), with thinking that remains highly dependent on rules and authority; in terms of morality, they tend to evaluate behaviour based on adults' approval rather than on principles of independent autonomy.⁵⁵ In the Confucian cultural context, this natural developmental dependence is further reinforced by social and moral norms. Therefore, although children from age seven may understand consent, their independence in making legally significant decisions remains limited and is strongly influenced by their parents. On that basis, under the LPDP in Vietnam, the requirement to obtain the simultaneous consent of both parents and children aged seven and over is, in practice, neither appropriate nor culturally grounded, and thus lacks substantive effectiveness.

In the educational environment, where personal data processing for enrolment, academic records, health management, and teaching primarily serves the student's own interests, a scenario in which the child withholds consent while the legal representative grants it would, under a strict reading of dual consent, produce conflicts that are difficult to resolve in practice. Given that Vietnamese cultural and legal structures already vest parents with both moral authority and representative capacity, the child's consent is, in many cases, consultative rather than dispositive; insisting on co-equal legal weight thus complicates implementation without enhancing substantive protection. Accordingly, in cases of genuine conflict, the decision of the legal representative, charged with safeguarding the best interests of the child, should be regarded as final, while the views of the child are weighed in accordance with age and maturity, rather than formalistically absolutised.

53 Pham Diem, ‘Relationships between Parents and Children under Vietnam's Ancient Laws’ [2011] Vietnam Law and Legal Forum <<https://vietnamlawmagazine.vn/relationships-between-parents-and-children-under-vietnams-ancient-laws-4343.html>> accessed 27 March 2026.

54 Thi Bich Hang Nguyen, ‘The Concepts of Filial Piety and Factors Affecting Filial Piety of Vietnamese People’ (2025) 67(2) VMOST Journal of Social Sciences and Humanities 117, doi:10.31276/VMOSTJOSSH.2024.0064.

55 Martha Lally and Suzanne Valentine-French, ‘Kohlberg's Stages of Moral Development’ in Martha Lally and Suzanne Valentine-French, *Lifespan Development: Psychological Perspective* (College of Lake County Foundation 2022) 373; Roger JR Levesque, *Adolescence, Privacy, and the Law: A Developmental Science Perspective* (OUP 2016) <<https://doi.org/10.1093/acprof:oso/9780190460792.001.0001>>.

3.2.3. Suspension of children's personal data processing

Article 24(3) LPDP makes suspension turn on the withdrawal of consent or on intervention by a competent authority where the child's interests are at risk.⁵⁶ On its face, this embodies the revocability of consent, treating control over a child's data as something that can always be reclaimed rather than permanently surrendered. Yet the provision leaves unresolved the question that the dual structure makes unavoidable, namely, whose withdrawal triggers suspension.

In the context of dual consent, a notable question arises: whether suspension is triggered by the withdrawal of one party alone or requires the withdrawal of both parties. A maximum-protection reading, under which withdrawal by either party would convert the mechanism into a unilateral veto, disrupting essential sectors such as education and healthcare; the converse reading, requiring both to withdraw, contradicts the revocability of consent and weakens protection. The underlying problem is that the law does not clarify whether dual consent comprises two independent expressions of will of equal value or whether the children's consent is consultative alongside that of the legal representative. In the absence of detailed guidance, equating the legal weight of a child with that of a representative, without a priority rule, risks creating practical conflicts, particularly in educational settings where data processing is necessary to perform public functions.

Furthermore, the mechanism also empowers competent authorities to order the cessation of processing where there are sufficient grounds to fear harm to the child's interests. This confirms that valid consent does not legitimise every processing activity. The legislator thus adopts a preventive stance, permitting intervention before actual harm occurs, in recognition that children cannot protect themselves.⁵⁷ However, the effectiveness and reasonableness of this provision depend on clearly defining the standard of "sufficient grounds" to avoid abuse of administrative intervention powers, yet such criteria currently lack specific guidance. This poses the risk that suspending processing may harm the best interests of the subjects being protected.

56 The processing of children's personal data shall be suspended when the person who has given consent withdraws the consent permitting the processing of children's personal data, except where otherwise provided by law or at the request of a competent authority where there are sufficient grounds to demonstrate that the processing of personal data may infringe upon the lawful rights and interests of the child. See, Law of Vietnam No 91/2025/QH15 (n 4) art 24(3).

57 *ibid*, art 24(3)(b); European Commission, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679* (Article 29 Data Protection Working Party, WP 248 rev.01, adopted 4 October 2017, last revised 4 October 2017) <<https://ec.europa.eu/newsroom/article29/items/611236/en>> accessed 17 April 2026.

3.2.4. Sanctions for Infringements of Children's Personal Data

With respect to sanctions imposed for infringing on children's personal data, these have been relatively clearly provided for in the Vietnamese legal system. Accordingly, violations involving the infringement of children's personal information in cyberspace may be subject to administrative sanctions or incur criminal liability, depending on the severity of the violation.

1) Administrative sanctions.

Administrative sanctions are applied in a tiered manner between organisations and individuals, and calibrated to the nature, severity, and economic impact of the violation. For organisations, Article 8(5) of the LPDP sets a general maximum monetary fine of VND 3 billion for violations of personal data protection.⁵⁸ However, for certain particularly serious violations, this Law applies a mechanism for calculating fines based on a percentage or on the unlawful gains. Accordingly, for unlawful cross-border transfer of personal data, the maximum fine may reach up to 5% of the total revenue of the preceding financial year;⁵⁹ in cases where the organisation has no revenue or where the fine calculated based on revenue is lower than VND 3 billion, the maximum of 3 billion shall apply. For buying and selling personal data, the maximum fine is set at ten times the amount of unlawful gains obtained from the violation;⁶⁰ if such gains cannot be determined or if the calculated amount is lower than VND 3 billion, the maximum of VND 3 billion shall also apply. This mechanism shows that the legislator not only sanctions the violation itself but also deprives unlawful economic beneficiaries,⁶¹ thereby preventing situations in which violations are profitable. Individuals committing the same violations face fines at half the organisation's rate, reflecting differentiated liability. Beyond administrative sanctions, criminal acts are subject to prosecution under the Criminal Code, and damages are compensable. The design thus combines strong deterrence of serious violations, such as illegal transfers or trading, with a transparent ceiling under Article 8(5).

Currently, the Ministry of Public Security is in the final stages of drafting a Decree on administrative penalties in the fields of cybersecurity and personal data protection.⁶² However, when assessing the consistency between the LPDP and the Draft Decree, there are significant technical discrepancies regarding the determination of fine levels.

58 Law of Vietnam No 91/2025/QH15 (n 4) art 8(5).

59 *ibid*, art 8(4).

60 *ibid*, art 8(3).

61 See, by analogy, Regulation (EU) 2016/679 (n 72) art 83, which establishes a two-tier fine structure reaching up to 4% of total worldwide annual turnover: Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) doi:10.1093/oso/9780198826491.001.0001.

62 Thi Thuy Duong Phan, Thi Than Niem Tran and Duc Giang Pho, 'Draft Decree Dealing with Violations of Personal Data Protection Regulations' (*PwC Vietnam Legal NewsBrief*, 10 May 2024) <<https://www.pwc.com/vn/en/publications/2024/240510-draft-pdpd.pdf>> accessed 25 May 2026.

The most significant question concerns fines for serious violations. Article 8 LPDP sets the maximum fine, which may reach up to 5% of total revenue⁶³ of the preceding financial year for unlawful cross-border transfers, up to ten times the unlawful gains for the trading of personal data and VND 3 billion general ceiling otherwise, a design intended to eliminate economic incentives for infringement and to deter large enterprises. The Draft Decree, however, has progressed through two stages regarding this architecture. Earlier drafts diverged sharply from the parent law, confining the revenue-based fine to narrow conditions, omitting the multiplier mechanism for unlawful data trading, and retaining low fixed brackets for breach-notification failures, a configuration that risked diminishing deterrence and contravening the principle that subordinate legislation must not weaken the effect of the parent law. The most recent draft has substantially closed this gap, lowering the quantitative threshold for cross-border violations, restoring the multiplier mechanism for unlawful data trading, and replacing the low fixed brackets with a tiered scheme.⁶⁴ The trajectory of the drafting process is itself revealing. The initial divergence and its subsequent correction show that the deterrent architecture of Article 8 LPDP is not self-executing but depends on the political will sustained through the subordinate legislation that operationalises it.

2) Criminal sanctions.

In Vietnam, the protection of personal data, including children's data, is governed not only by administrative measures but may also result in criminal sanctions for serious violations.

Criminal liability attaches under two provisions of the Criminal Code 2015. Article 159 reaches unauthorised access to or disclosure of private correspondence, and Article 288 reaches the unlawful provision or use of information on computer networks.⁶⁵ Neither provision, however, was drafted with children in mind. Both treat the victim's age as irrelevant to the offence and at most as a discretionary aggravating factor, so the criminal regime offers no child-specific protection and reaches children's data only incidentally, through offences designed for the general population.

63 Law of Vietnam No 91/2025/QH15 (n 4) art 8.

64 Earlier drafts confined the revenue fine to cases involving more than 5,000,000 citizens and omitted the multiplier mechanism. The latest draft applies the 3%–5% revenue fine to cases involving 1,000,000 citizens or more (Article 70(3)), restores fines of two to ten times the unlawful gains up to VND 3 billion for unlawful data trading (Article 67), and establishes a tiered regime reaching VND 60 million for reporting delays beyond 72 hours and VND 80 million for failure to implement remedial measures (Article 68).

65 Article 159 carries fines of VND 20–50 million, non-custodial reform of up to three years, or imprisonment of six months to three years, rising to five years for serious consequences. Article 288 carries fines of VND 30–200 million or imprisonment of six months to three years, rising to seven years for organised offences, dangerous recidivism, or the loss of critical data, with further aggravation where national security, social order, or the victim's life is affected. See, Law of Vietnam No 100/2015/QH13 'Criminal Code' (adopted 27 November 2015) <<https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Bo-luat-hinh-su-2015-296661.aspx>> accessed 17 April 2026.

Criminal sanctions, with severe penalties such as imprisonment and fines, play an important role in deterring serious violations of the right to privacy and personal data, including children's data. Moreover, criminal sanctions ensure that grave violations of victims' rights, particularly children, are adjudicated with fairness and transparency. The application of imprisonment and supplementary measures serves to prevent recidivism and protect society from similar criminal conduct.

3.3. Children's Data Protection Framework under the GDPR

In this section, the GDPR is utilised as a comparative framework to identify regulatory gaps in Vietnamese law regarding the protection of children's personal data. Rather than treating the GDPR merely as an external legal model for benchmarking, this section focuses on regulatory techniques that offer instructive insights for Vietnam, particularly in three dimensions: (i) a progressive and revenue-linked sanctioning regime; (ii) an independent supervisory authority model; and (iii) a specialised set of rules for children regarding consent, transparency, and data protection by design. These three dimensions not only reflect the GDPR's advanced development in safeguarding children in the digital environment but also provide a basis for a systematic assessment of the gaps identified in subsections 3.2.1–3.2.4, thereby informing recommendations for Vietnam.

These three areas should not be assessed in isolation. The strength of the European model lies in the way its components reinforce one another. A strong sanctioning regime has limited value without an independent authority capable of enforcing it, just as an age threshold remains weak if it is not supported by meaningful consequences for non-compliance. Examining Vietnam's framework in separate fragments would therefore miss precisely what makes the original model function as a coherent regulatory system.

First, the sanctioning of the GDPR under Article 83 is built upon two principles directly relevant to the law reform discussion in Vietnam. The first principle is the graded severity of penalties. Article 83(4) prescribes a lower maximum fine of up to 10 million EUR or 2% of the total worldwide annual turnover, whichever is higher, for violations concerning procedural and technical security obligations, including data breach notification duties under Articles 33–34 and data protection impact assessment requirements under Article 35. Conversely, Article 83(5) establishes a higher maximum fine of up to 20 million EUR or 4% of the total worldwide annual turnover for infringements related to core data processing principles, the lawfulness of processing, data subjects' rights, and international data transfer regulations.

The second principle is revenue sensitivity. By tethering the upper limit of penalties to a percentage of global turnover rather than a fixed monetary amount, the GDPR ensures that sanctions retain their deterrent effect even when the infringing entity is a multinational company with revenue that far exceeds any fixed statutory ceiling.

Furthermore, Article 83(2) mandates supervisory authorities to determine the specific fine amount based on eleven distinct criteria (points a to k), including the nature and gravity of the infringement, the categories of personal data affected, the degree of cooperation exhibited by the infringer, and any previous infringements. Crucially, through the open-ended criterion of any other aggravating or mitigating factor under point k, infringements affecting vulnerable subjects, such as children's data, are treated as an aggravating circumstance. This mechanism successfully reconciles the requirement of deterrence with the principle of proportionality. The Vietnamese drafting process itself shows why this element of the GDPR model is transferable. Article 8 LPDP incorporates a revenue-based fine ceiling. While earlier versions of the Draft Decree risked undermining this mechanism by confining it too narrowly, the latest revisions have largely realigned it with the LPDP, thereby preserving the deterrent architecture of the sanctioning regime.

Second, the independent supervisory authority model under Articles 51–59 of the GDPR establishes a reference benchmark for the structural separation between personal data protection and general policing or security functions. Each Member State must designate one or more public authorities responsible for monitoring the application of the GDPR pursuant to Article 51. These authorities must operate with complete independence when performing their tasks in accordance with Article 52. The members of these authorities remain free from external influence, a status safeguarded through fixed tenures, professional qualification requirements, and budgetary autonomy.

The tasks of supervisory authorities under Article 57 are broadly designed to encompass issuing guidelines, handling complaints, conducting investigations, approving certification mechanisms, and advising on legislative measures. The corrective powers under Article 58 include issuing warnings and reprimands, imposing bans on data processing, and imposing administrative fines. Notably, this model is further reinforced at the constitutional level by Article 8(3) of the Charter of Fundamental Rights of the EU, which explicitly mandates that compliance with data protection rules shall be subject to control by an independent authority.

The cooperation and consistency mechanisms under Articles 60–67, together with the EDPB under Articles 68–76, extend this institutional logic to cross-border cases. This is particularly relevant for Vietnam, as the most significant violations involving children's data are often tied to foreign digital platforms. This is the dimension on which the gap is widest. Vietnam's supervisory function sits inside the Ministry of Public Security, the very type of security-oriented body from which the GDPR model deliberately separates oversight, so the problem for Vietnam is not the absence of an authority but the absence of independence within the one it already has.

Third, the GDPR contains a specialised set of regulations concerning children. These provisions constitute a relatively comprehensive regulatory technique for the processing of children's data. Recital 38 establishes the foundational principle that children merit specific protection because they may be less aware of the risks and safeguards associated with the

processing of their data. This Recital also highlights specific contexts of concern, such as marketing, profiling, and services offered directly to children.

This principle is operationalised through five closely interrelated groups of regulations. The conditions for lawfulness under Article 6 must be satisfied for all data processing activities. When consent serves as the legal basis, the qualitative requirements of Article 7 apply: consent must be freely given, specific, informed, and unambiguous; the data controller must demonstrate that such consent was given; and the withdrawal of consent must be equally as easy. Article 8 establishes a specialised consent for children regarding information society services offered directly to them. Accordingly, if the child is below the applicable age threshold, the processing of data requires authorisation from the holder of parental responsibility. Concurrently, the data controller is obligated to make reasonable efforts to verify such authorisation, taking into account available technology. The transparency obligations under Articles 12–14 are heightened by Article 12(1). This provision stipulates that any information addressed to children must be presented in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. This standard is further developed in the EDPB's Guidelines 03/2022 on Deceptive Design Patterns.⁶⁶ Article 25 imposes binding obligations regarding data protection by design and by default. The data controller must implement appropriate technical and organisational measures to integrate data protection principles into the processing operations. Simultaneously, they must ensure that, by default, only personal data necessary for each specific purpose is processed. This provision is crucial for default privacy settings, the data minimisation principle, and the restriction of profiling targeting children. Article 35 requires a data protection impact assessment for processing activities that are likely to pose a high-risk to data subjects' rights. Under the EDPB's approach, this high risk threshold is generally met when children's data are processed on a large scale or for behavioural targeting.

The deterrent efficacy of these regulations is currently observable in practice. The decisions of the Irish Data Protection Commission against TikTok in 2023⁶⁷ and Meta/Instagram in 2022⁶⁸, both of which centred on the application of Articles 5, 12, 13, and 24–25 to children,

66 EDPB, *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them* (version 2.0, adopted 14 February 2023) <https://www.edpb.europa.eu/documents/guideline/guidelines-032022-on-deceptive-design-patterns-in-social-media-platform_en> accessed 17 April 2026.

67 EDPB, *Binding Decision 2/2023 on the Dispute Submitted by the Irish SA Regarding TikTok Technology Limited (Art 65 GDPR)* (adopted 2 August 2023) <https://www.edpb.europa.eu/documents/edpb-binding-decisions/binding-decision-22023-on-the-dispute-submitted-by-the-irish-sa_en> accessed 17 April 2026.

68 Data Protection Commission, *Decision in the Matter of Meta Platforms Ireland Limited, Formerly Facebook Ireland Limited, and the "Instagram" Social Media Network* (DPC Inquiry Reference: IN-20-7-4, adopted 2 September 2022) <<https://www.dataprotection.ie/en/dpc-guidance/decisions/inquiry-concerning-processing-personal-data-relating-child-users-instagram-social-networking-service>> accessed 17 April 2026.

demonstrate that the specialised obligations for children under the GDPR can compel major digital entities to alter their design choices. Vietnam possesses none of this layer. It has no child-specific transparency standard, no data protection by design obligation, and no DPIA requirement for children's data, so the protective burden falls entirely on a consent rule that, as Section 3.2.2 showed, the cultural context already weakens.

Across these dimensions, Vietnam has borrowed substantive form but still lacks key institutional and design conditions that make the European model effective. Although recent revisions to the Draft Decree have successfully restored the sanctioning ceiling, the supervisory authority exists but lacks independence, and the child-specific layer remains absent altogether. These three modes of incomplete transfer, the half-adopted, the misplaced, and the missing, define the reform agenda that Section 4 takes up in turn, in each case calibrated to the constitutional and socio-cultural conditions analysed above.

4 RECOMMENDATIONS FOR IMPROVING VIETNAMESE LAW

The gaps identified in the preceding sections do not call for a wholesale importation of the European model but for reforms calibrated to the conditions under which Vietnamese law operates. Each of the four proposals below addresses one of those gaps, and each is governed by the question that has run through this article: namely, how far a borrowed rule can be made to work once it enters a different legal and cultural setting.

First, determining age and the consent mechanism for children in the processing of personal data is a fundamental issue in children's data protection law, as it concerns the balance between two values: the protection of children and respect for children's autonomy as data subjects. Therefore, the design of the consent mechanism cannot be purely technical; it must be grounded in the theoretical foundations of children's developmental capacity, the best interests of the child, and Vietnam's socio-cultural characteristics.

European experience is instructive here. Article 8 GDPR sets the default age of digital consent at sixteen and permits Member States to derogate to a minimum age of thirteen, resulting in a fragmented European landscape. This heterogeneity has been criticised by the EDPB and the Fundamental Rights Agency as undermining the consistency of children's protection across the internal market. More importantly, treating children of thirteen and above as fully capable of giving consent on their own creates a protection gap for the thirteen to seventeen age group, who remain "children" under UNCRC and are the cohort most exposed to risks in the digital environment. Simultaneously, this model is inconsistent with the principle of evolving capacities, which posits that a child's maturity is not uniform and must be recognised in stages.⁶⁹ Conversely, if all decision-

69 Convention on the Rights of the Child (n 14) art 5; UN CRC, *General Comment No 25 (2021)* (n 41) para 19. See also, Lina Jasmontaite and Paul De Hert, 'The EU, Children Under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet' (2015) 5(1) *International Data Privacy Law* 20, doi:10.1093/idpl/ipu029.

making power is assigned to the legal representative until close to the age of majority without recognising the voice of the child, there is a risk of going against the modern approach that considers children as rights-holders who have the right to participate in decisions concerning them. Therefore, both extreme approaches, either premature autonomy or absolute paternalism, fail to achieve the necessary balance.

In Vietnam, this issue must be viewed through a cultural lens influenced by Confucianism and traditional village social structures. The philosophy of “filial piety” and hierarchical order in the family reinforces the guiding role of parents over children, and village culture, with the close linkage between family honour and community, resulting in children having a higher degree of dependence on parental will, which can be compared to many Western societies. However, Confucianism is not merely a system of authority; it also emphasises the principle of harmony, advocating for the avoidance of extremes and the pursuit of balance between values.⁷⁰

On this basis, it is proposed that provisions on age and consent mechanisms be amended toward a stratified approach as follows:

- 1 For children under seven years of age. All decisions relating to the processing of personal data shall be made by the legal representative. This is a stage at which children do not yet have the capacity to independently perceive digital risks; assigning full decision-making authority to the representative is consistent with the reality of psychological development.
- 2 For children aged from seven to under sixteen years. The position advanced here is not the wholesale adoption or rejection of a dual consent mechanism, but rather its risk stratification. The consent of the legal representative remains in every case a mandatory legal condition for processing. What varies is whether the child’s own consent is additionally required. For processing that poses heightened risks to the child’s legitimate rights and interests, the child is given not a co-equal role in authorising the processing, but a limited negative control through which an objection may halt it. For routine processing that directly serves the child’s educational, health, or welfare interests, enrolment, academic records, school health management, ordinary medical care, and comparable activities, the representative may decide independently, provided the child is informed with age-appropriate explanations and consulted in a manner commensurate with their cognitive level; the child’s view operates here as a consultative input rather than as a co-equal legal condition, reflecting the cultural and developmental realities analysed in Section 3.2.2. For high-risk processing, by contrast, the representative’s consent should be supplemented by a qualified right of the child to object, because the child’s independent voice acquires genuine protective value where processing engages risks of a different order.

70 Bedford and Yeh (n 51) 100.

The differential treatment of these two categories of processing follows from a feature of the cultural pressure analysed above. That pressure does not bear symmetrically on the two directions in which a child may express their will. Norms of filial piety, hierarchical order within the family, and community observation tend to place children in a position of deference to parental will rather than encouraging them to voice opposition. This is not to suggest that the family is the only source of such pressure. Children are also influenced by peers, schools, digital platforms, and online communities. In decisions concerning data processing, however, where the legal representative occupies the central legal role, the dominant direction of pressure remains one of deference.

In such a context, a child's consent and a child's refusal should not be assumed to carry the same epistemic value. When a child consents, genuine volition is difficult to distinguish from conformity to social norms. This signal is therefore less reliable and, for that reason, should not be granted coequal legal weight in routine processing. A child's active refusal does not always reflect an accurate perception of risk. A child may object out of fear, misunderstanding, or a failure to appreciate longer-term benefits. Yet because such a refusal must run against the prevailing tendency towards deference, it carries cautionary value. It therefore warrants more serious consideration than consent alone.

On this basis, the mechanism proposed for high-risk processing is not dual consent in the sense of treating the child's consent as a constitutive condition equal to that of the legal representative. The consent of the legal representative remains the principal legal condition for processing. What is added is a qualified right of the child to object, carrying suspensive effect and a duty of reassessment. This right is not conferred because the child has attained full autonomy, a proposition already rejected in Section 3.2.2. It is conferred because, where processing carries a serious risk of harm to a child's privacy, honour, psychological development, digital identity, or future opportunities, a signal of objection from the very person affected should be capable of suspending the processing and triggering an obligation to reassess it. The mechanism thus prevents processing from continuing, even when the legal representative's consent alone is sufficient, when it is the child who bears its direct consequences.

Understood in this way, a child's objection is neither a final and absolute legal decision nor an unconditional veto. It operates as a risk-control mechanism, functioning as a safety valve. It serves a preventive purpose while avoiding the risk that a child might permanently block processing that genuinely serves their own interests.

The weight accorded to this signal of objection should be calibrated to the child's age, maturity, and cognitive capacity, in line with the stratified framework proposed above. For younger children, an objection should be understood as an indication requiring the legal representative and the data controller to reassess. For older children, particularly those approaching sixteen, a refusal may carry greater legal weight. It then approaches the degree of self-determination that the framework proposed in this study recognises for children in the field of personal data processing. It does not amount to full civil-law capacity in the general sense.

Confining this mechanism to high-risk processing is proportionate to its institutional cost. In routine processing that directly serves a child's educational, health, or welfare interests, a right to object with suspensive effect, if applied indiscriminately, would disrupt essential services while generally offering no commensurate protective benefit. The boundary between the two categories is not fixed by the nominal label of an activity. Where processing described as routine, such as AI-based monitoring of academic performance, psychological profiling of students, location tracking, or the sharing of health data with third parties, in fact gives rise to a high-risk by reason of the nature of the data, the scale of processing, or its consequences for the child, it must be classified as high-risk processing and attract the child's right to object.

Drawing on Article 35(3) GDPR and EDPB Guidelines WP248 rev.01,⁷¹ processing should be classified as high-risk where it presents one or more of the following features: (a) public disclosure or dissemination of the child's data, including on social media platforms; (b) cross-border transfers to jurisdictions without an adequate level of protection; (c) processing of sensitive categories of data (health used beyond ordinary care, biometrics, religious belief, sexual orientation); (d) processing for commercial-profiling, behavioural advertising, or AI-training purposes; (e) systematic monitoring or large-scale processing; or (f) deployment of innovative technologies whose risks to the child are not yet well understood.

Second, children aged sixteen and above shall be entitled to decide independently whether to consent to or refuse the processing of personal data.⁷² At this age, children possess the capacity to understand and relatively fully evaluate the risks and consequences of data sharing in the digital environment. The selection of the age of sixteen is consistent with Article 8 of GDPR, according to which children's personal data processing in relation to information society services is lawful only where the child is at least 16 years old; below this age, processing is lawful only with the consent of the holder of parental responsibility.

This tiered approach not only addresses the limitations of the thirteen-year-old model but also mitigates the risk of absolutising the representative's role. It recognises children as evolving subjects of rights, while maintaining the necessary protective role of parents and providing the State with a clear legal basis for intervention when data-processing risks infringe upon children's rights.⁷³

In addition, it is necessary to supplement the mandatory data protection impact assessment (DPIA) for all processing activities that target children aged sixteen and

71 European Commission, *Guidelines* (n 57).

72 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation, GDPR) [2016] OJ L 119/1, art 8; OECD, *How's Life for Children in the Digital Age?* (OECD Publishing 2025) doi:10.1787/0854b900-en.

73 Lievens and Verdoodt (n 31).

over, particularly in high-risk sectors such as social networks, online games, educational technology (EdTech), and AI systems for behavioural profiling. A DPIA must specifically assess the impact on children's rights, not merely conduct a general assessment applied to adult users.⁷⁴

Third, drawing on European two-tier sanctioning architecture and on the analysis of Article 8 LPDP,⁷⁵ it can be affirmed that the orientation of strengthening sanctions under a two-tier model, linked to revenue ratios and unlawful gains, is consistent with modern legislative trends, but needs to be technically refined to ensure consistency and feasibility in the Vietnamese context. Article 8 LPDP installs a total-revenue-based architecture comparable in design to Article 83 GDPR, and although earlier drafts narrowed its operation through high quantitative thresholds and low fixed fines, the latest draft has largely realigned with the parent law. The remaining task is therefore not to restore deterrence, which the latest revisions have substantially achieved, but to entrench it, so that future amendments cannot quietly reopen the gap that the drafting process has just closed.

Consequently, the sanctioning mechanism should be enhanced to achieve a clear stratification of violation groups, such as the European Union's two-tiered ceiling model, but adjusted to Vietnam's socio-economic conditions. The group involving procedural, administrative, or technical security obligations may be subject to a general ceiling; whereas the group involving violations of fundamental data processing, processing without a legal basis, data trading, illegal overseas transfers, or serious infringements of children's data should be categorised under the highest sanction tier, applying revenue-based penalties or multiples of illicit turnover as stipulated in Article 8 of the LPDP.⁷⁶ Simultaneously, to ensure feasibility and prevent discretionary application, a system of guiding criteria should be added to determine specific fines within the brackets, including the nature, duration, and scope of the violation, the degree of cooperation, recidivism, and the financial scale of the enterprise.

In parallel with administrative sanctions, the refinement of criminal penalties should be considered selectively, focusing on organised acts, those aimed at significant illicit profits, or those causing severe consequences, rather than arbitrarily expanding criminalisation. A sanctioning mechanism designed in a properly tiered manner, maintaining the economic deterrence spirit of the LPDP, with clear technical guidance and consistency between the LPDP and the Decree, will not only enhance enforcement effectiveness but also affirm the

74 Simone van der Hof and Eva Lievens, 'The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR' (2018) 23(1) Communications Law 33; Regulation (EU) 2016/679 (n 72) art 35.

75 Law of Vietnam No 91/2025/QH15 (n 4) art 8; 'Draft Decree on Administrative Sanctions in the Field of Cybersecurity and Personal Data Protection' (n 12).

76 See, Regulation (EU) 2016/679 (n 72) art 83(4)–(5), which imposes ceilings of EUR 10 million or 2% of total worldwide annual turnover for procedural infringements, and EUR 20 million or 4% for substantive violations of data subjects' rights.

position of personal data protection, particularly children's data, as a legal value subject to strict protection within the Vietnamese legal system.

Fourth, building on the analysis of Articles 51–59 of the GDPR and Article 8(3) of the EU Charter, Vietnam should establish a specialised supervisory authority for personal data protection, modelled after the Data Protection Authorities (DPAs) found in many jurisdictions, particularly within the EU.⁷⁷ Beyond sanctioning, such an authority would issue guidance and interpretations, resolve complaints, conduct inspections, perform DPIAs, and formulate policy recommendations. In the Vietnamese context, where children's personal data is increasingly exploited online, a specialised authority would enhance the consistency of enforcement and enable early detection of infringements.

Currently, the competent authority for personal data protection is the Ministry of Public Security, a model that offers centralisation and rapid investigative capacity, but one in which placing management, inspection, and sanctioning within an authority whose primary mandate is security and public order carries two risks. First, the independence and objectivity of oversight may be subordinated to cybersecurity management priorities, preventing privacy protection from being fully realised as an independent value.⁷⁸ Second, a security-oriented approach risks overshadowing the human rights dimension, whereas personal data protection is, in essence, a fundamental personality right that requires a balance between state administration and individual liberty.

The relevant question for Vietnam is therefore not whether the authority can be made independent of the Government, which its constitutional structure does not readily allow, but whether it can be made independent of the security apparatus, since it is the latter, not the former, that compromises objective oversight. Vietnam should therefore consider establishing a specialised supervisory authority with relative independence, potentially placed under the Government, empowered to issue binding guidance, conduct independent inspections, apply administrative sanctions under the LPDP, and prioritise the protection of vulnerable groups such as children.

Implementation could proceed in two stages. In the first, a Personal Data Protection Commission would be established under the Government, drawing part of its initial staff from the Ministry of Public Security but governed by fixed-term appointments and a separate budget, with the Ministry retaining only the criminal-investigation function. This

77 Kuner and others (n 61) art 52, doi:10.1093/oso/9780198826491.003.0093; Thi Tuyet Dung Thai, Van Duong Nguyen and Van Lam Nguyen, 'A Comparative Study of Cross-Border Data Transfer Regulations in Vietnam and Singapore: Ensuring the Protection of Privacy' (2025) 26(2) *Asia-Pacific Journal on Human Rights and the Law* 81, doi:10.1163/15718158-26020001.

78 See, Regulation (EU) 2016/679 (n 72) art 52(1)–(2) requiring supervisory authorities to 'act with complete independence' and remain 'free from external influence'; Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, art 8(3); Thi Thu Huynh, 'Everyone Is Safe Now: Constructing the Meaning of Data Privacy Regulation in Vietnam' (2024) 11(4) *Asian Journal of Law and Society* 530, doi:10.1017/als.2024.36.

separates administrative supervision from criminal enforcement without dismantling existing capacity. In the second stage, once institutional competence is consolidated, the Commission would assume independent sanctioning power and cross-border enforcement competence. A domestic precedent exists in the National Competition Commission, which operates within the Ministry of Industry and Trade, yet follows a distinct adjudicative procedure, indicating that Vietnam has already accepted a semi-independent regulator within a ministry. This would overcome the current fragmentation of competences and affirm that personal data protection is not merely a matter of cybersecurity but a core element of human rights protection in a rule-of-law state.⁷⁹

Fifth, the Government of Vietnam should promote policies to develop and apply data protection technologies for children's personal data, imposing obligations on data collectors and controllers to provide clear, age-appropriate transparency before children aged sixteen and above make consent decisions. Studies show that children online are data subjects whose information is shared, collected, and processed without their understanding of the consequences.⁸⁰ Therefore, notices regarding processing purposes, the scope of third-party sharing, retention periods, and the right to withdraw consent must be presented in language tailored to the cognitive capacity of minors. Articles 12 and 25 GDPR, read with the EDPB's Guidelines 03/2022 on dark patterns, require that information directed to children be provided in clear and plain language and that privacy-protective settings apply by default, standards that materially improve children's capacity to understand and control what they are consenting to. Building on principles of data protection by design and privacy by default, Vietnam should adopt minimum technical security standards for systems processing children's data, including child-friendly interface design, encryption in transit and at rest, access control and audit logging, security monitoring, and periodic risk assessments, together with incentives and technical support for online education platforms, games, and digital services targeting children. Complementary measures should include child-specific privacy tools, content filters, alert applications, and educational programmes on information security risks to enhance children's capacity for self-protection in cyberspace.

Sixth, it is necessary to enhance publicity and transparency in the enforcement of children's personal data protection regulations. Selective disclosure of information regarding serious violations, accompanied by the resulting sanctions, will establish important legal precedents and raise societal awareness of the dangers of infringing upon children's data. However, such

79 Milkaite and Lievens (n 1) 1.

80 Cansu Caglar, 'Children's Right to Privacy and Data Protection: Does the Article on Conditions Applicable to Child's Consent under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?' (2021) 12(2) European Journal of Law and Technology 1; Stoilova, Nandagiri and Livingstone (n 26) 557.

disclosure must adhere to the principle of victim protection, ensuring that no additional information is disclosed that could lead to the child's identification.⁸¹

Furthermore, given the cross-border nature of personal data and digital services, Vietnam must participate in and strengthen international cooperation regarding children's personal data. This includes learning from nations with advanced legal systems and oversight mechanisms, while participating in and internalising international treaties and standards on privacy and data protection. This approach will not only help Vietnam keep pace with global trends but also provide the legal and systemic basis to coordinate the handling of children's data violations involving foreign elements.⁸²

5 CONCLUSIONS

Children's personal data protection has emerged as an imperative in Vietnam's digital transformation, serving not only to safeguard privacy but also to uphold human rights and the holistic development of children. Although Vietnam's current legal framework, most notably the LPDP 2025, has established a relatively comprehensive foundation, significant limitations persist in consent mechanisms, age thresholds, and sanctions for protecting children's privacy and personal data. This paper's contribution to comparative legal scholarship is a framework of culturally conditioned legal transfer: rather than transplanting the GDPR wholesale or rejecting it as foreign, each borrowed element, age thresholds, consent architecture, sanctioning tiers, supervisory design, is calibrated against the receiving jurisdiction's socio-cultural structure (Confucian filial hierarchy and the "Lang" community order) and the child's evolving capacities. This reframes the transplant-versus-particularism debate into a graduated inquiry: which features of a foreign regime are culturally portable, which require structural adaptation, and which must be designed indigenously. The study is doctrinal and comparative; it does not examine enforcement practice or how the proposed model would operate in Vietnamese schools, clinics, or EdTech platforms.

81 Ingrida Milkaite and Eva Lievens, 'Child-Friendly Transparency of Data Processing in the EU: From Legal Requirements to Platform Policies' (2020) 14(1) *Journal of Children and Media* 5, doi:10.1080/17482798.2019.1701055.

82 OECD, *Recommendation of the Council on Children in the Digital Environment* (OECD Legal Instruments, OECD Publishing 2021). See also, UN CRC, *General Comment No 25 (2021)* (n 41) paras 122–124, on international cooperation.

REFERENCES

1. Bedford O and Yeh KH, 'The History and the Future of the Psychology of Filial Piety: Chinese Norms to Contextualized Personality Construct' (2019) 10 *Frontiers in Psychology* 100, doi:10.3389/fpsyg.2019.00100
2. Caglar C, 'Children's Right to Privacy and Data Protection: Does the Article on Conditions Applicable to Child's Consent under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?' (2021) 12(2) *European Journal of Law and Technology* 1
3. Diem P, 'Relationships between Parents and Children under Vietnam's Ancient Laws' [2011] *Vietnam Law and Legal Forum* <<https://vietnamlawmagazine.vn/relationships-between-parents-and-children-under-vietnams-ancient-laws-4343.html>> accessed 27 March 2026
4. Grimes SM, 'Responsible AI and Children: Towards a Rights-Based Approach to AI Governance' (*Sesame Workshop, Joan Ganz Cooney Center*, 23 January 2025) <<https://joanganzcooneycenter.org/2025/01/23/responsible-ai-and-children/>> accessed 3 February 2026
5. Hof S and Lievens E, 'The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR' (2018) 23(1) *Communications Law* 33
6. Hof S and others, 'The Child's Right to Protection Against Economic Exploitation in the Digital World' (2020) 28 *The International Journal of Children's Rights* 833, doi:10.1163/15718182-28040003
7. Huynh TT, 'Everyone Is Safe Now: Constructing the Meaning of Data Privacy Regulation in Vietnam' (2024) 11(4) *Asian Journal of Law and Society* 530, doi:10.1017/als.2024.36
8. Jasmontaite L and De Hert P, 'The EU, Children Under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet' (2015) 5(1) *International Data Privacy Law* 20, doi:10.1093/idpl/ipu029
9. Julija A, 'Most Worrying Identity Theft Statistics for 2026' (*Fortunly*, 27 March 2026) <<https://fortunly.com/statistics/identity-theft-statistics/>> accessed 7 February 2026
10. Kim D, 'The Concept of Filial Piety in East Asian Confucian Culture from the Perspectives of Gadamer and Habermas' (2019) 33-34 *Kritika Kultura* 36
11. Kuner C and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) doi:10.1093/oso/9780198826491.001.0001
12. Lally M and Valentine-French S, 'Kohlberg's Stages of Moral Development' in Lally M and Valentine-French S, *Lifespan Development: Psychological Perspective* (College of Lake County Foundation 2022) 373

13. Lâm TT, 'Protect Children's Rights from Cyberviolence under the Vietnamese Law' (2025) 8(3) *International Journal of Innovative Research and Scientific Studies* 2689, doi:10.53894/ijirss.v8i3.7070
14. Le TKD, 'Characteristics of Traditional Vietnamese Family and Its Influence on Communication Culture in the Family' (2021) 1(11) *Anthropological Researches and Studies* 49, doi:10.26758/11.1.4
15. Leijten EL and Hof S, 'Dissecting the Commercial Profiling of Children: A Proposed Taxonomy and Assessment of the GDPR, UCPD, DSA and AI Act in Light of the Precautionary Principle' (2025) 57 *Computer Law & Security Review* 106143, doi:10.2139/ssrn.5055046
16. Levesque RJR, *Adolescence, Privacy, and the Law: A Developmental Science Perspective* (OUP 2016) <<https://doi.org/10.1093/acprof:oso/9780190460792.001.0001>>
17. Lievens E and Verdoodt V, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34(2) *Computer Law & Security Review* 269, doi:10.1016/j.clsr.2017.09.007
18. Livingstone S and others, 'Children's Privacy in the Digital Age: US and UK Experiences and Policy Responses' in Christakis DA and Hale L (eds), *Handbook of Children and Screens: Digital Media, Development, and Well-Being from Birth Through Adolescence* (Springer 2025) 491, doi:10.1007/978-3-031-69362-5_67
19. Livingstone S and others, 'Children's Rights and Online Age Assurance Systems: The Way Forward' (2024) 32 *International Journal of Children's Rights* 721, doi:10.1163/15718182-32030001
20. Livingstone S, Stoilova M, and Nandagiri R, *Children's Data and Privacy Online: Growing Up in a Digital Age* (LSE Media and Communications 2019)
21. Macenaite M and Kosta E, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) *Information & Communications Technology Law* 146, doi:10.1080/13600834.2017.1321096
22. Milkaite I and Lievens E, 'Child-Friendly Transparency of Data Processing in the EU: From Legal Requirements to Platform Policies' (2020) 14(1) *Journal of Children and Media* 5, doi:10.1080/17482798.2019.1701055
23. Milkaite I and Lievens E, 'Children's Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm' (2019) 10(1) *European Journal of Law and Technology* 1
24. Milkaitė I and Mačėnaitė M, 'Advancing Children's Privacy and Data Protection Rights: Emerging Data Protection Trends and Challenges in Selected CEE Countries' in Limantė A and Vaičiūnienė R (eds), *Children's Rights in Central and Eastern Europe: A Comparative Analysis with a Spotlight on Lithuania* (Springer 2025) 325, doi:10.1007/978-3-032-07092-0_16

25. Montgomery KC and Chester J, 'Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework' (2015) 1(4) *European Data Protection Law Review* 277, doi:10.21552/EDPL/2015/4/6
26. Nguyen Q, 'Vietnam Fares Poorly in Online Child Safety Ranking' *VnExpress International* (Hanoi, 15 February 2020) <<https://e.vnexpress.net/news/news/vietnam-fares-poorly-in-online-child-safety-ranking-4053720.html>> accessed 1 February 2026
27. Nguyen TBH, 'The Concepts of Filial Piety and Factors Affecting Filial Piety of Vietnamese People' (2025) 67(2) *V MOST Journal of Social Sciences and Humanities* 117, doi:10.31276/VMOSTJOSSH.2024.0064
28. Nyst C, Geary P, and Gorostiaga A, *Privacy, Protection of Personal Information and Reputation Rights* (Discussion Paper Series: Children's Rights and Business in a Digital World, UNICEF 2017)
29. Persano F, 'GDPR and Children Rights in EU Data Protection Law' (2020) (spec) *European Journal of Privacy Law & Technologies* 32
30. Phan TTD, Tran TTN, and Pho DG, 'Draft Decree Dealing with Violations of Personal Data Protection Regulations' (*PwC Vietnam Legal NewsBrief*, 10 May 2024) <<https://www.pwc.com/vn/en/publications/2024/240510-draft-pdps.pdf>> accessed 25 May 2026
31. Quynh LHC, 'The Influences of Collectivism on Vietnamese Communication Style' (2021) 4(7) *International Journal of Research in Engineering, Science and Management* 10
32. Radesky J and others, 'Digital Advertising to Children' (2020) 146(1) *Pediatrics* e20201681, doi:10.1542/peds.2020-1681
33. Radesky J and others, 'Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children' (2022) 5(6) *JAMA Network Open* e2217641, doi:10.1001/jamanetworkopen.2022.17641
34. Rossi A and others, 'Who Is Vulnerable to Deceptive Design Patterns? A Transdisciplinary Perspective on the Multi-Dimensional Nature of Digital Vulnerability' (2024) 55 *Computer Law & Security Review* 106031, doi:10.1016/j.clsr.2024.106031
35. Rozendaal E and Buijzen M, 'Children's Vulnerability to Advertising: An Overview of Four Decades of Research (1980s–2020s)' (2023) 42(1) *International Journal of Advertising* 78, doi:10.1080/02650487.2022.2135349
36. Schäfer R and others, 'Growing Up with Dark Patterns: How Children Perceive Malicious User Interface Designs' (NordCHI 24: 13th Nordic Conference on Human-Computer Interaction, Uppsala, Sweden, 13-16 October 2024) doi:10.1145/3679318.3685358
37. Smyr D and Ulianova E, 'Legal Issues of Children's Personal Data Protection' (2022) 5(1) *Open Journal for Legal Studies* 1, doi:10.32591/coas.ojls.0501.01001s

38. Soenens B and others, 'The Moderating Role of Vertical Collectivism in South-Korean Adolescents' Perceptions of and Responses to Autonomy-Supportive and Controlling Parenting' (2018) 9 *Frontiers in Psychology* 1080, doi:10.3389/fpsyg.2018.01080
39. Sofian A and others, 'Children's Privacy and Data Protection in Judicial Decisions in Indonesia' (2021) 18(4) *US-China Law Review* 153, doi:10.17265/1548-6605/2021.04.001
40. Stoilova M, Nandagiri R, and Livingstone S, 'Children's Understanding of Personal Data and Privacy Online: A Systematic Evidence Mapping' (2021) 24(4) *Information, Communication & Society* 557, doi:10.1080/1369118X.2019.1657164
41. Thai TTD, Nguyen VD, and Nguyen VL, 'A Comparative Study of Cross-Border Data Transfer Regulations in Vietnam and Singapore: Ensuring the Protection of Privacy' (2025) 26(2) *Asia-Pacific Journal on Human Rights and the Law* 81, doi:10.1163/15718158-26020001
42. Verdoodt V and Lievens E, 'Targeting Children with Personalised Advertising: How to Reconcile the (Best) Interests of Children and Advertisers' in Vermeulen G and Lievens E (eds), *Data Protection and Privacy under Pressure: Transatlantic Tensions, EU Surveillance and Big Data* (Maklu 2017) 313
43. Yim EPY, 'Effects of Asian Cultural Values on Parenting Style and Young Children's Perceived Competence: A Cross-Sectional Study' (2022) 13 *Frontiers in Psychology* 905093, doi:10.3389/fpsyg.2022.905093

AUTHORS' INFORMATION

Thi Tuyet Dung Thai

Ph.D, Associate Professor, Legal Affairs Department, Vietnam National University Ho Chi Minh City (VNU-HCM), Vietnam

dungttt@uel.edu.vn

<https://orcid.org/0000-0002-5570-2988>

Co-author, responsible for Supervision, Conceptualisation, Methodology, Validation, and Writing – review & editing.

Van Duong Nguyen*

LL.M, Faculty of Economic Law, University of Economics and Law, Vietnam National University Ho Chi Minh City (VNU-HCM), Vietnam

duongnv@uel.edu.vn

<https://orcid.org/0009-0001-6494-7549>

Corresponding author, responsible for Conceptualisation, Methodology, Project administration, Formal analysis, Investigation, Writing – original draft, and Writing – review & editing.

Van Lam Nguyen

LL.B, Legal Affairs Department, Vietnam National University Ho Chi Minh City (VNU-HCM),
Vietnam

nvlam.ttpc@vnuhcm.edu.vn

<https://orcid.org/0009-0007-8891-4120>

Co-author, responsible for Investigation, Resources, Data curation, Formal analysis, Validation, and Writing – review & editing.

Competing interests: The authors declare no competing interests. No financial, personal, or professional relationships that could have influenced the research, analysis, or conclusions of this manuscript have been disclosed.

Disclaimer: The views and opinions expressed in this manuscript are solely those of the authors and do not represent the views, policies, or positions of any affiliated institutions, organisations, or funding bodies.

RIGHTS AND PERMISSIONS

Copyright: © 2026 Thi Tuyet Dung Thai, Van Duong Nguyen and Van Lam Nguyen. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

EDITORS

Managing editor – Mag. Bohdana Zahrebelna. **English Editor** – Robert Reddin.

Ukrainian language Editor – Liliia Hartman.

ABOUT THIS ARTICLE

Cite this article

Thai, TTD, Nguyen VD and Nguyen VL, 'Protection of Children's Privacy and Personal Data: A Perspective from Vietnamese Law' (2026) 9(3) Access to Justice in Eastern Europe 500-35 <<https://doi.org/10.33327/AJEE-18-9.3-a0002000>>

DOI: <https://doi.org/10.33327/AJEE-18-9.3-a0002000>

Summary: 1. Introduction. – 2. Methodology. – 3. Results and Discussion. – 3.1. *Children, Children's Personal Data, and Children's Personal Data Protection.* – 3.2. *The current state of the legal framework on children's personal data protection in Vietnam.* – 3.3. *Children's Data Protection Framework under the GDPR.* – 4. Recommendations for Improving Vietnamese Law. – 5. Conclusions.

Keywords: *Children's personal data protection; Informed consent; GDPR; Vietnamese data protection law; Confucian legal culture.*

ADDITIONAL INFORMATION

This research is funded by Vietnam National University Ho Chi Minh City (VNU-HCM) under a project within the framework of the Program titled “Strengthening the capacity for education and basic scientific research integrated with strategic technologies at VNU-HCM, aiming to achieve advanced standards comparable to regional and global levels during the 2025-2030 period, with a vision toward 2045”.

DETAILS FOR PUBLICATION

Date of submission: 25 Apr 2026

Date of acceptance: 23 Jun 2026

Online First Publication: 23 Jul 2026

Last Publication: 05 Aug 2026

Was the manuscript fast-tracked? - No

Number of reviewer reports submitted in the first round: 2 reports

Number of revision rounds: 1 round with major revisions

Technical tools were used in the editorial process

Plagiarism checks - Turnitin from iThenticate

<https://www.turnitin.com/products/ithenticate/>

Scholastica for Peer Review

<https://scholasticahq.com/law-reviews>

AI DISCLOSURE STATEMENT

This article was prepared with the assistance of AI tools. Specifically, Grammarly and Quillbot were employed for proofreading during the drafting process (version reviewed: June 2026). The authors confirm that all content, arguments, and conclusions were generated independently and remain their sole responsibility. No AI tool was used for generating original research findings or analysis.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ЗАХИСТ КОНФІДЕНЦІЙНОСТІ ТА ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ: ПЕРСПЕКТИВА В'ЄТНАМСЬКОГО ЗАКОНОДАВСТВА

Тхі Туєт Дунг Тай, Ван Дуонг Нгуєн* та Ван Лам Нгуєн

АНОТАЦІЯ

Вступ. Захист персональних даних дітей стає нагальним питанням у В'єтнамі та в усьому світі. У цій статті аналізується правова основа захисту персональних даних дітей у В'єтнамі та розглядається конкретне правове питання про те, наскільки В'єтнам може впровадити правові елементи, що наразі викладені в Загальному регламенті про захист даних (GDPR). У статті визначено структурні обмеження щодо вікових порогів, механізмів згоди, санкцій та органу із захисту персональних даних. У статті також пропонуються рекомендації та пропозиції у сфері державної політики щодо вдосконалення в'єтнамського законодавства про захист даних, зокрема модель визначення віку надання згоди, диференційовану відповідно до рівня розвитку дитини, та спеціалізований наглядовий орган, з ширшою метою забезпечення безпечного цифрового середовища, орієнтованого на розвиток дітей.

Методи. У цій статті застосовуються різноманітні методи правового дослідження, що поєднують три підходи: 1) доктринальний правовий аналіз для визначення, інтерпретації та оцінки нормативної бази В'єтнаму; 2) функціональний порівняльний аналіз для порівняння в'єтнамського законодавства з GDPR, для оцінки ступеня їхньої сумісності та визначення регуляторних механізмів, які можуть бути імplementовані у в'єтнамське законодавство; та 3) міждисциплінарний контекстуальний аналіз, що спирається на психологію розвитку, міжкультурну психологію та правову антропологію, для оцінки здатності дітей ухвалювати рішення, структури сімейної ієрархії та впливу конфуціанської етики та культури «Ланг» на стосунки між батьками та дітьми, що дає змогу отримати висновки, необхідні для адаптації міжнародних моделей до В'єтнаму. Вторинні джерела, включно з рецензованими науковими роботами та звітами міжнародних організацій, дозволяють інтерпретувати отримані результати у ширшому контексті.

Результати та висновки. Хоча В'єтнам розробив основоположну систему правового регулювання, суттєві недоліки стосуються: 1) визначення «дитини» та вікові порогові згоди є непослідовними та недостатньо узгодженими з розвитком здібностей дітей; 2) механізми подвійної згоди та призупинення не мають чіткості та погано узгоджуються з культурними чинниками, що асиметрично послаблюють згоду дитини порівняно з її правом заперечити; 3) режим санкцій не забезпечує належного превентивного ефекту, незважаючи на нещодавні законодавчі зміни; та 4) В'єтнаму не стільки бракує наглядового органу, скільки незалежного: його наглядова функція наразі

знаходиться в апараті безпеки, водночас він не має зобов'язань щодо прозорості, адаптованої до потреб дитини, захист даних за замовчуванням і на етапі проектування або оцінки впливу на захист даних (DPIA). На цій основі у статті пропонується концепція культурно зумовленого правового трансферу, яка класифікує кожен механізм GDPR як такий, що може бути застосований у незмінному вигляді, потребує структурної адаптації або вимагає розробки власного (національного) механізму, та пропонує: (а) багаторівневу модель згоди з кваліфікованим правом дитини заперечувати проти обробки даних з високим рівнем ризику; (б) прозорість, орієнтовану на дітей, захист даних на етапі проектування (data protection by design) та обов'язкову оцінку впливу на захист даних (DPIA); (в) диференційовану систему санкцій, що залежить від рівня доходів; (г) спеціалізований орган із захисту даних із відносною незалежністю та компетенцією у сфері трансграничного правозастосування; (д) прозорість процедури надання згоди, адаптовану до вікових особливостей; (е) поглиблене міжнародне співробітництво. Ці пропозиції реформ враховують конституційний лад та соціокультурний контекст В'єтнаму.

Ключові слова. Захист персональних даних дітей; інформована згода; GDPR; в'єтнамське законодавство про захист даних; конфуціанська правова культура.

TÓM TẮT BẰNG TIẾNG VIỆT*

Bài báo nghiên cứu

BẢO VỆ QUYỀN RIÊNG TƯ VÀ DỮ LIỆU CÁ NHÂN CỦA TRẺ EM: GÓC NHÌN TỪ PHÁP LUẬT VIỆT NAM

Thái Thị Tuyết Dung, Nguyễn Văn Dương, Nguyễn Văn Lâm

TÓM TẮT

Bối cảnh: Bảo vệ dữ liệu cá nhân của trẻ em đang trở thành một vấn đề cấp thiết tại Việt Nam cũng như trên phạm vi toàn cầu. Bài viết này phân tích khung pháp lý của Việt Nam về bảo vệ dữ liệu cá nhân của trẻ em và giải quyết câu hỏi pháp lý cụ thể là Việt Nam có thể tiếp nhận đến đâu những khía cạnh pháp lý đang được quy định trong GDPR. Bài viết chỉ ra những hạn chế mang tính cấu trúc bao gồm: ngưỡng độ tuổi, cơ chế đồng ý, chế tài và cơ quan bảo vệ dữ liệu cá nhân. Sau cùng, bài nghiên cứu đề xuất các kiến nghị, gợi mở nhằm hoàn thiện pháp luật Việt Nam, bao gồm mô hình độ tuổi đồng ý phân tầng theo mức độ phát triển và một cơ quan giám sát chuyên trách, với mục tiêu chung là bảo đảm một môi trường số an toàn và định hướng phát triển cho trẻ em.

*The publication metadata in Vietnamese is presented as submitted by the author.

Phương pháp: Bài viết được thực hiện trên cơ sở nghiên cứu pháp lý định tính với cách tiếp cận đa phương pháp. (i) phương pháp phân tích pháp luật thực định được sử dụng nhằm nhận diện, giải thích và đánh giá hệ thống pháp luật hiện hành của Việt Nam; (ii) phương pháp so sánh chức năng được vận dụng để đối chiếu pháp luật Việt Nam với GDPR, để đánh giá mức độ tương thích và xác định các kỹ thuật điều chỉnh có thể tiếp nhận. (iii) bài viết sử dụng cách tiếp cận liên ngành, kết hợp các luận điểm của tâm lý học phát triển, tâm lý học xuyên văn hóa và nhân học pháp luật để lý giải năng lực ra quyết định của trẻ em, cấu trúc quyền uy trong gia đình, cũng như ảnh hưởng của đạo đức Nho giáo và văn hóa làng xã đối với quan hệ cha mẹ - con cái. Những yếu tố này có ý nghĩa quan trọng trong việc đánh giá khả năng tiếp nhận và cấy ghép các mô hình pháp lý quốc tế nhằm phù hợp với bối cảnh Việt Nam. Nghiên cứu cũng sử dụng các nguồn tài liệu thứ cấp, bao gồm các công trình khoa học đã qua phản biện và báo cáo của các tổ chức quốc tế, nhằm hỗ trợ cho quá trình phân tích.

Kết quả và Kết luận: Mặc dù Việt Nam đã thiết lập một khung pháp lý nền tảng, vẫn tồn tại những hạn chế đáng kể: (i) định nghĩa "trẻ em" và các ngưỡng độ tuổi đồng ý còn thiếu nhất quán và chưa được quy định phù hợp với năng lực phát triển của trẻ em; (ii) cơ chế đồng ý kép và đình chỉ xử lý chưa rõ ràng và chưa tương thích với áp lực văn hóa vốn làm suy yếu một cách bất đối xứng giá trị của sự đồng ý so với sự phản đối của trẻ; (iii) tính rủi ro của chế tài còn chưa thực sự hiệu quả mặc dù đã được điều chỉnh gần đây; và (iv) Việt Nam không thiếu một cơ quan giám sát mà thiếu một cơ quan độc lập do chức năng giám sát hiện đặt trong bộ máy an ninh, đồng thời chưa có các nghĩa vụ về minh bạch dành riêng cho trẻ em, bảo vệ dữ liệu ngay từ khâu thiết kế, hay đánh giá tác động xử lý dữ liệu.

Trên cơ sở đó, bài viết đề xuất một khung lý thuyết về chuyển giao pháp luật có điều kiện về văn hóa, phân loại mỗi kỹ thuật của GDPR thành: có thể tiếp nhận nguyên trạng, cần điều chỉnh về cấu trúc, hoặc phải thiết kế nội sinh; và kiến nghị: (a) mô hình đồng ý phân tầng kèm theo quyền phản đối có điều kiện của trẻ đối với hoạt động xử lý có rủi ro cao; (b) minh bạch dành riêng cho trẻ em, bảo vệ dữ liệu ngay từ khâu thiết kế, và đánh giá tác động dữ liệu bắt buộc; (c) cơ chế chế tài phân tầng, gắn với doanh thu; (d) cơ quan bảo vệ dữ liệu chuyên trách có tính độc lập tương đối và thẩm quyền thực thi xuyên biên giới; (e) minh bạch phù hợp với độ tuổi trong quá trình đồng ý; và (f) tăng cường hợp tác quốc tế. Những cải cách này cần được đặt trong giới hạn của nguyên tắc hiến định và điều kiện văn hóa - xã hội của Việt Nam, thay vì chỉ tiếp nhận cơ học các mô hình pháp lý từ bên ngoài.

Từ khóa: Bảo vệ dữ liệu cá nhân của trẻ em; sự đồng ý trên cơ sở được cung cấp thông tin; GDPR; pháp luật Việt Nam; văn hóa pháp lý Nho giáo.