In-Depth Research Report of Laws / Policies Related to Online Privacy of Children and Adolescents Including Social Perception Survey

APEC Digital Economy Steering Group

November 2026

Asia-Pacific Economic Cooperation

Asia-Pacific
Economic Cooperation

In-Depth Research Report of Laws / Policies Related to Online Privacy of Children and Adolescents Including Social Perception Survey

Digital Economy Steering Group (DESG)

November 2026

APEC Project: DESG 202 2024A

Produced by

Project Overseer:
Personal Information Protection Commission (PIPC), Republic of Korea
Korea Internet & Security Agency (KISA)

Author:
Kyoungjin CHOI
Room 607 of Law Building, Gachon University
1342 Seongnamdaero
Republic of Korea 13120
Tel: (82) 31-750-8764
Email: kjchoi@gachon.ac.kr

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

© 2026 APEC Secretariat

APEC#226-CT-01.15

This report presents the findings of a research project conducted by the research team led by Kyoungjin Choi, Professor at the College of Law and Director of the Center for AI, Data and Policy at Gachon University, Republic of Korea.

Acknowledgement: Sincere appreciation is extended to Attorney Hyewon Han of Kim & Chang, Attorney Dayeon Ahn of Yulchon LLC who actively participated in the research team, and the representatives of APEC member economies who made significant contributions by providing valuable insights and information through the APEC workshop and various channels.

Table of contents

Summary 1

Chapter 1 Introduction 6

Section 1 Purpose of the Research Project 6

Section 2 Background and rationale of the project 6

Chapter 2 Regulatory Framework for the Protection of Children's and Adolescents' Personal Data 7

Section 1 The Overall Legal Framework Governing Children and Adolescents 7

I. Introduction 7

II. Status of APEC economies 7

III. Comparative Analysis and Implications 18

Section 2 Distinction Between Adults and Children and adolescents in Personal Data Laws: Key Categories and Regulations 20

I. Introduction 20

II. Status of APEC economies 20

III. Comparative Analysis and Implications 26

Section 3 Criteria and Scope of Personal Data Privacy Regulations for Children and Adolescents 28

I. Introduction 28

II. Status of APEC economies 28

III. Comparative Analysis and Implications 33

Section 4 Enforcement and Sanctioning Trends for Children and Adolescents' Personal Data Processing 35

I. Introduction 35

II. Status of APEC economies 35

III. Comparative Analysis and Implications 40

Chapter 3 Obligations for Privacy by Design (PbD) in Processing Children or Adolescents' Personal Data 43

Section 1. Privacy by Design Regulations for Children and Adolescents Services 43

I. Introduction 43

II. Status of APEC economies 43

III. Comparative Analysis and Implications 49

Section 2. Practical Implementation of Privacy by Design for Children and Adolescents 51
I. Introduction 51
II. Status of APEC economies 52
III. Comparative Analysis and Implications 54
Chapter 4 Age Assurance Obligations and Methods in Each Economy 57
Section 1 Applicability of Age Assurance to Non-Child-Directed Services 57
I. Introduction 57
II. Status of APEC economies 57
III. Comparative Analysis and Implications 61
Section 2 Specific Categories Subject to Strict Verification 62
I. Introduction 62
II. Status of APEC economies 63
III. Comparative Analysis and Implications 67
Section 3 Adopted Mechanisms for Age Verification 68
I. Introduction 68
II. Status of APEC economies 68
III. Comparative Analysis and Implications 72
Section 4 Non-Statutory Guidelines and Industry Practices for Age Verification 73
I. Introduction 73
II. Status of APEC economies 74
III. Comparative Analysis and Implications 77
Chapter 5 Separate Legal Bases Required for Processing Children or Adolescents' Personal Data 79
Section 1 Differentiating the Legal Grounds for Minors and Adults 79
I. Introduction 79
II. Status of APEC economies 79
III. Comparative Analysis and Implications 82
Section 2 Recognized Legal Bases for Processing Children's and Adolescents' Personal Data 84
I. Introduction 84
II. Status of APEC economies 84
III. Comparative Analysis and Implications 86

Section 3 Scope of Consenting Parties 88
I. Introduction 88
II. Status of APEC economies 88
III. Comparative Analysis and Implications 91
Section 4 Scope of Minors' Independent Consent 92
I. Introduction 92
II. Status of APEC economies 92
III. Comparative Analysis and Implications 95
Section 5 Regulation of Consent Verification Methods 96
I. Introduction 96
II. Status of APEC economies 96
III. Comparative Analysis and Implications 99
Section 6 Permissibility of Bundled (Comprehensive) Consent 100
I. Introduction 100
II. Status of APEC economies 101
III. Comparative Analysis and Implications 104
Chapter 6 Clear and Understandable Notice to Children or Adolescents 106
Section 1 Legal distinctions between adult and minors 106
I. Introduction 106
II. Status of APEC economies 106
III. Comparative Analysis and Implications 110
Section 2 Analysis of Corporate Practices and Case Studies 111
I. Introduction 111
II. Status of APEC economies 111
III. Comparative Analysis and Implications 114
Chapter 7 Children or Adolescents' "Rights" 116
Section 1. Children or Adolescents' "Rights" as data subjects 116
I. Introduction 116
II. Status of APEC economies 116
III. Comparative Analysis and Implication 123
Section 2. The "Right to be Forgotten" for Children and Adolescents 125
I. Introduction 125

II. Status of APEC economies 125
III. Comparative Analysis and Implication 132
Chapter 8 Prohibition of Certain Processing Purposes or Types of Personal Data Involving Children or Adolescents 135
Section 1. Profiling and Targeted Advertising Involving Children or Adolescents 135
I. Introduction 135
II. Status of APEC economies 135
III. Comparative Analysis and Implication 141
Section 2. Exploitative and Harmful Use of Children's Personal Data 142
I. Introduction 142
II. Status of APEC economies 143
III. Comparative Analysis and Implication 149
Section 3. Legal Mechanisms Enabling Children and Adolescents to Request the Takedown of Online Content 150
I. Introduction 150
II. Status of APEC economies 151
III. Comparative Analysis and Implication 155
Chapter 9 Self-Regulation by Companies and Government Support (Incentives, etc.) Regarding Children or adolescents Personal Data Protection 158
I. Introduction 158
II. Status of APEC economies 158
III. Comparative Analysis and Implications 161
Chapter 10 Conclusion 163
Policy Recommendations to Ensure Data Protection and Privacy of 168
Children and Adolescents in Online Space 168
Appendix A: Report of the Workshop Result 170
Appendix B: Social Perception Survey 170

[Table]

Table 1 Overall legal framework governing protection of child and adolescents 18
Table 2 Distinction Between Adults and Children and adolescents in Personal Data Laws 26
Table 3 Criteria and Scope of Personal Data Privacy Regulations for Children and Adolescents 33

Table 4 Enforcement and Sanctioning Trends for Children and Adolescents' Personal Data Processing 40
Table 5 Privacy by Design Regulations for Children and Adolescents Services 49
Table 6 Practical Implementation of Privacy by Design for Children and Adolescents..... 54
Table 7 Applicability of Age Verification to Non-Child-Directed Services 61
Table 8 Specific Categories Subject to Strict Verification 67
Table 9 Adopted Mechanisms for Age Verification 72
Table 10 Non-Statutory Guidelines and Industry Practices for Age Verification..... 77
Table 11 Differentiating the Legal Grounds for Minors and Adults..... 82
Table 12 Recognized Legal Bases for Processing Children's and Adolescents' Personal Data 87
Table 13 Scope of Consenting Parties..... 91
Table 14 Scope of Minors' Independent Consent 95
Table 15 Regulation of Consent Verification Methods..... 99
Table 16 Permissibility of Bundled (Comprehensive) Consent..... 104
Table 17 Legal distinctions between adult and minors..... 110
Table 18 Corporate Practices and Cases 114
Table 19 Children or Adolescents' "Rights" as data subjects 124
Table 20 The "Right to be Forgotten" for Children and Adolescents..... 132
Table 21 Profiling and Targeted Advertising Involving Children or Adolescents..... 141
Table 22 Exploitative and Harmful Use of Children's Personal Data 149
Table 23 Legal Mechanisms Enabling Children and Adolescents to Request the Takedown of Online Content..... 156
Table 24 Self-Regulation 162

Summary

Chapter 1 Introduction

- **Section 1. Purpose of the Research Project:** The report aims to establish an empirical foundation for a safer digital ecosystem by evaluating child privacy safeguards and identifying regulatory gaps across 21 APEC economies. Its ultimate goal is to deliver evidence-based policy recommendations that strengthen institutional capacities and harmonize regional approaches to protecting the digital rights of future generations.
- **Section 2. Background and Rationale of the Project:** The rapid expansion of the digital economy has exposed children to heightened privacy risks and emerging threats, yet significant disparities exist in legal frameworks across the region. To address these cross-border challenges, this project establishes a coordinated regional initiative aligned with APEC priorities to bridge regulatory gaps and enhance capacity for robust online child protection.

Chapter 2 Regulatory Framework for the Protection of Children's and Adolescents' Personal Data

- **Section 1. The Overall Legal Framework Governing Children and Adolescents:** Significant disparities in legal frameworks and age thresholds across APEC economies create complex compliance burdens for businesses and unequal protection for children in the borderless digital environment. Addressing this fragmentation requires a shift toward regional interoperability, focusing on the harmonization of age verification standards and the development of common principles to bridge regulatory gaps between privacy and safety.
- **Section 2. Distinction Between Adults and Children and adolescents in Personal Data Laws: Key Categories and Regulations:** The diverse age thresholds and consent mechanisms across APEC economies create significant compliance burdens for businesses and technical complexities in implementing dynamic consent flows. This regulatory fragmentation risks either restricting adolescents' access to digital resources through overly strict requirements or exposing them to data exploitation due to low thresholds. Moving forward, APEC economies may benefit from harmonizing Age Bands by encouraging a regional consensus on "tiered" protections that distinguish between young children (needing strict parental control) and adolescents (needing safety-by-design and guided autonomy).
- **Section 3. Criteria and Scope of Personal Data Privacy Regulations for Children and Adolescents:** The region's regulatory shift from "directed to children" to a broader "likely to be accessed" standard acknowledges children's presence on general platforms but imposes significant compliance burdens and legal uncertainty on cross-border businesses. This evolution forces platforms to implement age assurance for all users, raising technical costs and adult privacy concerns, while highlighting the inadequacy of "actual knowledge" standards that may incentivize willful blindness regarding child users.
- **Section 4. Enforcement and Sanctioning Trends for Children and Adolescents' Personal Data Processing:** The lack of harmonized, child-specific penalty tiers across APEC economies creates risks of under-enforcement and legal uncertainty, necessitating shared guidelines such as a "vulnerability multiplier" to ensure consistent deterrence. While regulators increasingly treat child vulnerability as an aggravating factor leading to stricter operational remedies like service blocking, these practices should be formalized into statutory frameworks to guarantee robust protection. Codifying these factors would bridge

the gap between discretionary enforcement and the need for clear mandates that effectively penalize violations involving minors.

Chapter 3 Obligations for Privacy by Design (PbD) in Processing Children or Adolescents' Personal Data

- **Section 1. Privacy by Design regulations for children and adolescents' services:** This section assessed whether APEC economies require the integration of Privacy by Design (PbD) at the service design stage. The analysis found uneven regulatory approaches across the region: while some economies mandate PbD or child-specific impact assessments, many rely on general principles that allow broad discretion and result in inconsistent levels of protection.
- **Section 2. Practical Implementation of Privacy by Design for Children and Adolescents:** This section examined how PbD principles are applied in practice. Although documented examples remain limited, voluntary PbD initiatives are emerging through corporate practices, regulatory guidance, and industry self-regulation. These include default high-privacy settings, age assurance mechanisms, parental controls, and data minimization. However, the discretionary and uneven nature of voluntary adoption highlights the need for clearer regional guidance and cooperative frameworks.

Chapter 4 Age Verification Obligations and Methods in Each Economy

- **Section 1. Applicability of Age Verification to Non-Child-Directed Services:** This section examined whether general age verification requirements apply to services not specifically targeting minors. The analysis found that most economies limit such obligations to child-directed services, sector-specific contexts, or age-restricted content, with few adopting broader mandates. This cautious approach reflects concerns regarding proportionality and data minimization, while indicating an emerging expectation for privacy-preserving age assurance where child protection depends on age thresholds.
- **Section 2. Specific Categories Subject to Strict Verification:** This section analyzed age verification obligations in high-risk sectors. While economy-wide mandates remain uncommon, sector-specific requirements are widely and consistently enforced in areas such as adult content, gambling, gaming, and age-restricted goods. These obligations are typically grounded in sectoral or criminal law, reflecting a risk-based regulatory approach.
- **Section 3. Adopted Mechanisms for Age Verification:** This section reviewed the age verification methods recognized across APEC economies. The analysis identified substantial variation, with many jurisdictions prescribing no specific methods and others relying primarily on government-issued identification. Some economies permit or encourage alternative approaches, including third-party verification, payment-based authentication, biometric tools, and AI-based age estimation. The lack of harmonized standards highlights the need for proportionate, privacy-preserving, and risk-based guidance.
- **Section 4. Non-Statutory Guidelines and Industry Practices for Age Verification:** This section examined regulatory recommendations and voluntary corporate practices in the absence of legal mandates. Such practices remain limited and uneven, with only a small number of economies issuing non-binding guidance. In some cases, companies independently adopt age gates, parental controls, or monitoring mechanisms. These developments underscore the growing relevance of soft-law and industry-led approaches, while highlighting the need for clearer baseline guidance.

Chapter 5 Separate Legal Bases Required for Processing Children or Adolescents' Personal Data

- **Section 1. Differentiating legal grounds for minors and adults:** This section examined whether distinct legal bases apply to minors' data processing. The analysis found that most economies impose heightened requirements for minors—most commonly mandatory parental or guardian consent—reflecting concerns about minors' limited capacity for meaningful consent. The trend indicates a shift toward specialized legal regimes and away from adult-centric models.
- **Section 2. Recognized Legal Bases for Processing Children's and Adolescents' Personal Data:** This section analyzed the legal bases recognized for processing children's and adolescents' personal data. A strong consensus exists that consent from a legal representative is the primary lawful basis where a minor lacks capacity. Despite jurisdictional differences in implementation, this principle provides a common compliance foundation across the region.
- **Section 3. Scope of Consenting Parties:** This section examined who may consent on behalf of minors. Most economies restrict this authority to parents or legal guardians, emphasizing legal certainty and accountability. However, a minority allow context-specific alternatives, such as schools or representatives acting in the child's best interests, creating compliance challenges for cross-border services.
- **Section 4. Scope of minors' independent consent:** This section reviewed when minors may independently consent. The analysis found significant divergence: some economies require parental consent until adulthood, others apply fixed age thresholds, and others rely on case-by-case capacity assessments. These differences reflect varying balances between protection and autonomy and necessitate flexible, jurisdiction-sensitive compliance strategies.
- **Section 5. Regulation of consent verification methods:** This section examined how parental or guardian consent must be verified. The analysis revealed a sharp divide between jurisdictions relying on general standards of "reasonable" verification and those mandating specific, verifiable methods such as identity documents or authenticated signatures. This gap suggests potential weaknesses in enforcement and signals increasing expectations for robust verification mechanisms.
- **Section 6. Permissibility of Bundled (Comprehensive) Consent:** This section examined the necessity of prohibiting or restricting comprehensive consent for processing children's data. The analysis revealed that APEC economies employ varied approaches to the permissibility of bundled consent, highlighting the need for stricter and clearer criteria to ensure that consent obtained for minors' data is truly informed and specific.

Chapter 6: Clear and Understandable Notice to Children or Adolescents

- **Section 1. Legal distinctions between adult and minors:** This section reviewed legal obligations and specific requirements for providing age-appropriate privacy notices, considering the different legal standing of minors. The finding is that most APEC economies either legally mandate or recommend age-appropriate notice obligations, with a clear focus on ensuring minors can clearly understand their rights and the data processing policies.
- **Section 2. Analysis of Corporate Practices and Case Studies:** This involved analyzing the practical methods and case studies adopted by companies to make privacy notices clear and comprehensible for children and adolescents. Corporate practices

show a trend toward using simplified language, visual aids, and layered notices to enhance comprehension, which highlights best practices for effective communication with minors.

Chapter 7: Children or Adolescents' Rights

- **Section 1. Children or adolescents' Rights as data subjects:** The analysis covered some jurisdictions' recognition of data subject rights for children and adolescents and the relationship between their rights and the role of parents or guardians. Rights are increasingly recognized in certain jurisdictions, though in the event a jurisdiction recognizes those rights, a balance must be struck between the minor's independent capacity and the legal representative's role, with the analysis highlighting the variety in how APEC economies define this balance.
- **Section 2. The Right to be Forgotten for Children and Adolescents:** This section reviewed the legal recognition and practical initiatives regarding the 'Right to be Forgotten' specifically for children and adolescents. Legal frameworks and practical initiatives for the 'Right to be Forgotten' are present and evolving, particularly to address data posted by minors in their youth, emphasizing the importance of empowering children to manage their digital footprint.

Chapter 8: Prohibition of Certain Processing Purposes or Types of Personal Data Involving Children or Adolescents

- **Section 1. Profiling and Targeted Advertising Involving Children or Adolescents:** This section focused on the legal status of prohibiting or restricting personal data processing for profiling and targeted advertising aimed at minors. Significant efforts are being made across APEC economies to ban or strictly restrict the use of children's data for profiling and targeted advertising.
- **Section 2. Exploitative and Harmful Use of Children's Personal Data:** This section reviewed legal and regulatory measures to prevent the exploitative and harmful use of children's personal data, including AI-generated deepfake content. Stricter legal and regulatory measures are being adopted to combat exploitative uses, especially in response to the emerging threat of deepfake-based sexual content, indicating a focus on comprehensive technical and legal safeguards.
- **Section 3. Takedown Rights for Children and Adolescents:** The analysis covered the legal and practical frameworks ensuring specific 'Takedown Rights' (right to request deletion or cessation of use) for children and adolescents. Takedown rights are recognized as crucial for mitigating harm, with comparative analysis showing different procedural and substantive requirements across economies to facilitate the swift removal of harmful or unwanted content.

Chapter 9: Self-Regulation by Companies and Government Support (Incentives, etc.) Regarding Children or Adolescents Personal Data Protection

- This chapter examined the role of corporate self-regulation (codes of conduct, best practices) and government support/incentives for protecting children's personal data. Both corporate self-regulation and government support were found to be essential

components for fostering a culture of compliance and enhancing the effectiveness of overall data protection policies in the region.

Chapter 10: Social Perception Survey

- The social perception survey was conducted across seven APEC member economies to assess public awareness and identify key concerns regarding the protection of children's and adolescents' personal data. Although the findings are limited by a sample size heavily skewed toward Japanese respondents (accounting for approximately 86% of the 85 total responses), the data offers a valuable qualitative snapshot of current public sentiment. The results highlight a critical gap in public confidence regarding existing legal frameworks and enforcement, serving as a meaningful empirical reference for future policy discussions on enhancing digital safety for minors.

Appendix: Report of the Workshop Result

- The APEC workshop held in Incheon in July 2025 focused on "Ensuring Data Protection and Privacy of Children and Adolescents," discussing policy status and cooperation strategies across member economies. A survey revealed significant gaps in legal frameworks, age verification standards, and parental consent requirements among member economies. Experts from the 5Rights Foundation and Google emphasized "Privacy by Design (PbD)" and data minimization, calling for clear regulations and technical safeguards. Panel and small group discussions explored practical solutions, including effective age verification technologies, child-friendly privacy notices, and the guarantee of the "right to be forgotten". Participants expressed a strong consensus on the need for interoperable standards and common principles to overcome legal disparities between economies. Consequently, the workshop highlighted the essential need for continuous regional dialogue and a global framework to harmonize regulations. It also emphasized the importance of Korea's leadership and necessary domestic policy improvements, such as legislating the digital right to be forgotten.

Chapter 1 Introduction

Section 1 Purpose of the Research Project

The primary objective of this report is to lay the empirical and analytical foundation necessary for fostering a safer, more trusted, and child-appropriate digital ecosystem across the Asia-Pacific region. To achieve this, the research presents the findings of an in-depth survey and comparative analysis conducted across all 21 APEC member economies, offering a comprehensive evaluation of the current legal, policy, and regulatory safeguards protecting the online privacy and personal data of children and adolescents. Beyond merely mapping the existing landscape, this project aims to critically identify regulatory gaps, implementation challenges, and promising practices emerging within the region. Ultimately, the purpose of this report is to translate these analytical findings into evidence-based policy recommendations that will support APEC economies in strengthening their institutional capacities and harmonizing their approaches to digital safety for future generations.

Section 2 Background and rationale of the project

The rapid expansion of the digital economy in the Asia-Pacific region has deeply integrated digital platforms—ranging from social media to online gaming—into the daily lives of children and adolescents. While this connectivity offers significant educational and social benefits, it has simultaneously exposed young users to heightened privacy and safety risks, including indiscriminate data collection, profiling for targeted marketing, and emerging threats such as AI-generated deepfake content and online sexual exploitation. Despite these shared challenges, substantial differences remain among APEC economies regarding the maturity of their legal frameworks, particularly in critical areas such as age-appropriate design, parental consent mechanisms, and technical safeguards. Given the cross-border nature of digital services, individual domestic efforts are often insufficient, underscoring the urgent need for regional cooperation. Aligned with the priorities of APEC's Digital Economy Steering Group (DESG) and the Aotearoa Plan of Action, this project was established to bridge these regulatory divergences, facilitate the sharing of best practices consistent with domestic law, and build the necessary capacity to robustly protect the rights and well-being of children and adolescents online.

Chapter 2 Regulatory Framework for the Protection of Children's and Adolescents' Personal Data

The need to protect children and adolescents does not arise solely in the context of data privacy. Each economy may have regulatory frameworks for the protection of children and adolescents across various sectors, including content regulation, social media, gaming, etc. This section seeks to understand what comprehensive protective frameworks exist for children and adolescents beyond personal data laws, and how privacy regulations relate to these broader protections. Additionally, since children or adolescents vary in literacy and cognitive ability depending on age, the need for age-specific protection is important. This section aims to examine whether and how APEC economies have implemented stratified protections.

The following is an introduction and comparative analysis of the current regulatory systems of each APEC economy to suggest implications.

Section 1 The Overall Legal Framework Governing Children and Adolescents

I. Introduction

Before examining the specific laws and regulations regarding the protection of personal data of children and adolescents, this paper would like to first provide an overview of the entire legal system governing children and adolescents in order to understand the importance of the laws on children and adolescents in each economy. (e.g., Are there specific laws on personal data and privacy for children or adolescents? Do sector-specific laws, such as those related to gaming or child pornography, contain special provisions for the protection of children and adolescents?)

II. Status of APEC economies

1. Australia

In Australia, the *Privacy Act 1988* (Privacy Act) protects an individual's personal data regardless of their age.

Recent reforms to the Privacy Act require the Office of the Australian Information Commissioner (OAIC) to develop a Children's Online Privacy Code which will apply to social media and other online services likely to be accessed by children. This code will specify how the existing obligations in the Privacy Act will apply to children and may include additional requirements that aren't inconsistent with existing obligations. The OAIC is currently developing this code.

Note Australia uses the term ‘child abuse material’ not child pornography. The move to this wording was among amendments to Commonwealth legislation in 2019 to more accurately reflect the gravity of the crimes and the harm inflicted on victims.

States and Territories have primary responsibility to legislate on child sexual abuse matters in their jurisdiction. At the Commonwealth level the *Criminal Code Act 1995* (Criminal Code) includes a robust framework of offences that cover child abuse material offences committed via a carriage service (internet), a postal service or by Australian citizens or residents overseas. Subdivision 474.D offences include using a carriage service to access, transmit, solicit, etc. child abuse material. Subdivision 474.F offences include using a carriage service to engage with a child for sexual activity, to procure a child for sexual activity and to groom a child.

We note that the Department for Infrastructure, Transport, Regional Development, Communications, Sport & Arts (DITRDCA) may provide further information in relation to this question.

2. Brunei Darussalam

Until 2025, Brunei Darussalam had no legislation related to data privacy. In January 2025, Brunei Darussalam issued the Personal Data Protection Order. This order was introduced to give citizens greater control over how personal data is collected, used, and disclosed by private companies and non-governmental organizations (NGOs). However, it does not contain any provisions specifically related to children or adolescents.

3. Canada

There are no specific federal laws in Canada targeted exclusively at children and adolescents’ data privacy. Instead, general privacy frameworks apply to all individuals, including children and adolescents, and sector specific legislation (such as in healthcare and education) include additional provisions for children and adolescents. Additionally, guidance from data protection authorities offers further recommendations for safeguarding children and adolescents’ information.

4. Chile

The right to the protection of personal data is safeguarded as a constitutional fundamental right (Article 19, Paragraph 4 of the Constitution of the Republic of Chile).
The Privacy Protection Law (Ley 19628, Sobre protección de la vida privada) regulates the definition of personal data, its collection and processing, and the obligations of data controllers. However, it does not contain specific provisions for the enhanced protection of children and adolescents.

To address the limitations of the existing privacy law, Chile enacted a new Personal Data Protection Law (Ley 21719, Regula la protección y el tratamiento de los datos personales y crea la agencia de protección de datos personales) on 13 December 2024, which is scheduled to take effect on 1 December, 2026.
While the previous privacy law focused primarily on the protection of private life, the new law is regarded as a landmark piece of legislation for establishing a comprehensive framework for the protection of personal data.

5. People's Republic of China

The Provisions on the Protection of Children's Personal Information in Cyberspace, the independent regulations specifically dedicated to the protection of children's personal information, was unveiled in China in 2019. In addition, such protections are addressed within general personal information protection laws as well as general laws concerning children and adolescents.

- The Personal Information Protection Law (PIPL), China's dedicated legislation on personal data protection, classifies the personal data of children under the age of 14 as "sensitive personal data" (Article 28).
- Article 28 of the PIPL sets out three prerequisites for processing sensitive personal data: a specific purpose, sufficient necessity, and strict protective measures.
- Article 31 of the PIPL requires that "to process the personal information of minors under the age of 14, personal information processors shall obtain the consent of the parents or other guardians of the minors. Personal information processors processing the personal information of minors under the age of 14 shall develop special rules for processing such personal information.".
- The amended Law of the People's Republic of China on Protection of Minors (MPL), revised in June 2021, includes a dedicated chapter on internet protection, which contains special provisions for the protection of children's personal data.

This Children and adolescents Protection Law also stipulates that, in principle, the processing of personal data of children and adolescents under the age of 14 requires the consent of a parent or guardian, unless otherwise specified by other laws or administrative regulations.

Furthermore, based on this law, the Regulation on the Protection of Minors in Cyberspace was established to impose specific restrictions on the processing of personal data of children under the age of 14.

6. Hong Kong, China

In Hong Kong, China, the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") is a piece of technology-neutral and principle-based legislation. It is applicable to all sectors and all age groups, including children and adolescents.

Apart from the PDPO, the Prevention of Child Pornography Ordinance (Cap. 579) prohibits the production, possession and publication of child pornography; and the Control of Obscene and Indecent Articles Ordinance (Cap. 390) aims at protecting children and adolescents from the influence of harmful materials while maintaining free flow of information.

7. Indonesia

Indonesia’s most comprehensive data privacy law is the Personal Data Protection Law (PDP Law No. 27/2022), but it contains only limited provisions specifically addressing children and adolescents.
A broader law governing online information and transactions, the Electronic Information and Transaction Law (EIT Law), serves as the foundation for a more detailed regulation: Government Regulation No. 17 of 2025, regarding the Governance of Electronic System Implementation in Child Protection (“GR 17/2025”). This regulation provides the most specific and detailed rules for the protection of children’s and adolescents’ personal data.
In other words, while the PDP Law establishes general principles and rights concerning personal data, GR 17/2025 offers more concrete and practical guidelines for the protection of children’s data.

8. Japan

The protection of personal data is governed by the Act on the Protection of Personal data (APPI). The APPI guidelines provide explanations on how to obtain consent from children and adolescents; however, there are no specific provisions that distinguish the handling of children and adolescents' personal data and privacy from that of adults.

Meanwhile, certain individual laws set out age restrictions and age verification requirements in relation to the protection of children and adolescents. Examples include:

- Act on Regulation on Soliciting Children by Using Opposite Sex Introducing Service on Internet
  To prevent child prostitution and sex crimes, this law prohibits children and adolescents under the age of 18 from using dating websites.
- Juvenile Protection Ordinances enacted by prefectural governments
  In some prefectures, regulations impose restrictions such as limiting children and adolescents' access to smartphone games and social networking apps during nighttime hours and requiring age verification.

9. Republic of Korea

There isn't a separate, independent law specifically dedicated to the protection of personal data of children or adolescents. Instead, regulations concerning the personal data of children and adolescents are integrated into general personal data protection laws and related statutes.

According to the Personal Information Protection Act (“PIPA”), which is the general law concerning personal data protection:

- The state and local governments are required to implement policies necessary for the protection of personal data of children under 14 years of age (Article 5, Paragraph 3).
- To process the personal data of children under 14 years of age, consent from their legal guardian must be obtained. There's also a duty to confirm whether the legal guardian has consented and regulations regarding the method of notification to the child (Article 22-2).
- For children under 14 years of age, their legal guardian can exercise the data subject's rights, such as requesting access to the child's personal data (Article 38, Paragraph 2).

Additionally, according to the Act on the Protection and Use of Location Information (“Location Information Act”):

- Location information businesses and others must obtain consent from a legal guardian when collecting, using, or providing personal location data of children under 14 years of age, and they must verify that the legal guardian has consented (Article 25, Paragraph 1).
- Furthermore, for children aged 8 or younger, if a guardian who actually protects the child consents to the collection, use, and provision of personal location data for the protection of the child's life or body, it is considered as if the child has consented (Article 26).

Beyond personal data and information protection, there are also the following regulations aimed at protecting children or adolescents:

Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (“Network Act”) (Articles 41 to 42-3, etc.): This act contains provisions to protect children and adolescents from harmful information distributed through information and communication networks.

Act on the Protection of Children and Juveniles from Sexual Abuse: This law aims to protect children or adolescents from sexual offenses.

Juvenile Protection Act: This law aims to protect and rescue children and adolescents from harmful environments such as harmful media, drugs, and harmful businesses.

10. Malaysia

In Malaysia, the protection of children and adolescents is ensured through a combination of personal data protection laws and sector-specific regulations. The Personal Data Protection Act 2010 *[Act 709]* regulates the processing of personal data in commercial transactions and requires parental consent for children and adolescents under 18, although it does not have specific provisions for children or adolescents. The Personal Data Protection Department, under the Ministry of Digital, oversees the implementation of this Act.

For broader child protection, the Sexual Offences Against Children Act 2017 (Act 792) criminalizes child pornography and online sexual exploitation, enforced by the Royal Malaysia Police (PDRM) and the Attorney General's Chambers. The Ministry of Women,

Family and Community Development also plays a role in implementing policies related to child protection under this Act, overseeing the Domestic Children Policy and Malaysia's obligations under the Convention on the Rights of the Child (CRC), providing a comprehensive framework for protecting children and adolescents from exploitation and abuse.

Additionally, the Malaysian Communications and Multimedia Commission (MCMC), under the Communications and Multimedia Act 1998 (CMA), regulates and ensures the protection of children and adolescents from harmful online content, including the enforcement of age verification for access to adult material. These laws and agencies collectively work to safeguard the privacy and well-being of children and adolescents in Malaysia.

11. Mexico

Both the Federal Law for the Protection of Personal Data in Possession of Private Parties (LFPDPPP) and the General Law for the Protection of Personal Data in Possession of Obligated Subjects (LGPDPPSO), refer that the processing of personal data of children and adolescents must give priority to the best interests of the child and adolescent, in terms of the applicable legal provisions.

The Law for the Protection of Personal Data in Possession of Private Parties (LFPDPPP) does not provide for such an express provision.

However, in Mexico, the legal principle of the best interest of the child and adolescent means an obligation of public and private institutions, including judges and administrative authorities, to choose the option that best guarantees their physical, psychological, emotional, cultural, spiritual and social development and well-being. This includes ensuring their rights to life, survival, development, health, education, identity, family life, non-discrimination, freedom of expression and participation.

The legal principle of the best interest of the child and adolescent, is recognized in the General Law on the Rights of Children and Adolescents (LGDNNA) and is based on the Convention on the Rights of the Child (CRC), ratified by Mexico.

The laws that regulate certain conducts, even criminal ones, do not have specific sections on the protection of personal data of children and adolescents.

The aforementioned, in relation to general data protection provisions applicable to children and adolescents´ personal data.

It is relevant to highlight that there also are provisions directed at specific sectors such as the above mentioned.

12. New Zealand

The New Zealand Privacy Act applies to all individuals regardless of age. There are specific references for children under the age of 16 which provide additional privacy protection.

For example, when responding to an access request, an agency can refuse access to that information where the individual is under the age of 16 and disclosure of the information would be contrary to the interests of that individual (section 49(1)(c)).

Additionally, where a privacy breach has occurred, an agency is not required to notify a child under the age of 16 if the agency believes that the notification would be contrary to that individual's interests.

More generally, Information Privacy Principle 4 requires agencies to take extra care when collecting personal data from children and young people to ensure the manner of collection is fair and doesn't intrude to an unreasonable extent in the affairs of the individual concerned (Section 22, Information Privacy Principle 4 (b)(i) and (ii)).

13. Papua New Guinea

There is no general law that specifically addresses personal data protection in Papua New Guinea.
The Department of Information & Communications Technology has proposed a draft law titled the National Data Governance & Data Protection Policy 2024.
The Cybercrime Code Act 2016 regulates cybersecurity and internet-related crimes.

In addition, the draft Social Media Policy Concept Note proposed in 2025 by the Ministry of Information and Communication Technology includes specific provisions related to the personal data of children and adolescents. Among them is a provision that restricts children and adolescents' access to social media platforms.

Currently, there is virtually no legal framework in place for the protection of children's and adolescents' personal data. Since revisions to the proposed draft laws are still underway, it remains unclear what specific regulations will be enforced once these laws are implemented.

14. Peru

Peru's primary legislation on personal data protection is the Personal Data Protection Law No. 29733 (Ley de Protección de Datos Personales), which is based on Article 2 of the Peruvian Constitution.
This law affirms that all individuals, including children and adolescents, have the right to the protection of personal data concerning information that affects their private or family life.
The PDPL, together with the two regulations outlined below, forms the basis for understanding Peru's overall personal data protection framework.

Supreme Decree No. 003-2013-JUS – Regulation of the PDPL:
This decree was issued to further elaborate on the requirements of the PDPL and to establish more concrete and enforceable regulations.

Supreme Decree No. 016-2024-JUS, dated November 30, 2024:
This new regulation on personal data protection was introduced in response to the rapid advancement of e-commerce, artificial intelligence, and similar digital technologies. It includes improvements aimed at strengthening the defense of personal data protection.

Law 27489/2001, June 27, Regulating the Private Centres of Risk Information and Protection for the Owner Information:
A law related to the operation of private risk centers and personal data protection regulations.

15. The Republic of the Philippines

The Child and Youth Welfare Code (Presidential Decree No. 603) provides for the rights of children to protection, education, health, and moral development.

Sector Specific Laws

• Republic Act No. 7610, known as the "Special Protection of Children against Abuse, Exploitation, and Discrimination Act"

• Republic Act No. 9344, known as the "Juvenile Justice and Welfare Act of 2006"

• Republic Act No. 9775, known as the "Anti-Child Pornography Act of 2009" • Republic Act No. 11930, known as the "Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act"

These laws provide for specific provisions and mechanisms for the protection of children and adolescents and ensuring their welfare, including protection from abuse and exploitation, access to justice, and special protection in vulnerable situations. Furthermore, these laws contain confidentiality provisions designed to protect their identity and privacy in legal or criminal proceedings. This covers confidentiality of records and protection from undue publicity, as well as protective orders restricting access and prohibiting dissemination.

Likewise, the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti Child Sexual Abuse or Exploitation Materials (CSAEM) Act requires Internet Service Providers (ISPs) to establish high privacy setting as default safety and privacy settings for children, and where practicable and necessary, adopt age-verification controls and protocols to restrict their access to materials as may be classified by the Movie and Television Review and Classification Board.

Other laws

• Presidential Decree No. 1869, relative to the franchise and powers of the Philippine Amusement and Gaming Corporation (PAGCOR) prohibits persons under 21 years old and students from entering or playing in casinos and other gaming or gambling establishments.

• Republic Act No. 9211, known as the "Tobacco Regulation Act of 2003" prohibits the sale, distribution, and advertising of tobacco products to persons under 18 years old.

Privacy and Data Protection

• Children are recognized as data subjects with concomitant rights under the Data Privacy Act of 2012. The National Privacy Commission issued an Advisory on Guidelines on Child Oriented Transparency. Children as data subjects and rights holders are entitled to meaningful access to information. The Advisory provides guidelines for Personal data Controllers and Processors to ensure that children's personal data is processed with special care, emphasizing transparency, age-appropriate communication, and the best interests of the child.

16. The Russian Federation

In Russia, there is no standalone law specifically dedicated to the protection of children's personal data. Instead, all processing of personal data is governed by two general laws: Federal Law No. 152-FZ "On Personal Data" and Federal Law No. 149-FZ "On Information, Information Technologies and Protection of Information" (commonly referred to as the Information Law). However, the law titled "On Protecting Children from Information Harmful to Their Health and Development" (Federal Law No. 436-FZ, 2010) establishes a system for content classification and the restriction of harmful content, thereby indirectly contributing to the protection of children online.

17. Singapore

While Singapore's Personal Data Protection Act (PDPA) does not establish separate statutory provisions exclusively for children, Singapore has supplemented its general law framework with regulatory guidance tailored to children's personal data, which is considered a form of sensitive data regulated under the PDPA.

In particular, the PDPC's 2024 Advisory Guidelines on Children's Personal Data in the Digital Environment provide expectations on orgs handling children's data online, alongside guidance in the Selected Topics Advisory Guidelines.

In addition, there are other laws on online harms that seek to protect children. Singapore adopts a multi-layered regulatory approach, where children's data protection is addressed under the PDPA and PDPC's guidelines, while online harms are managed through separate legislation such as the Online Safety (Miscellaneous Amendments) Act 2022 and associated IMDA codes.

18. Chinese Taipei

The fundamental legal framework for personal data protection in Chinese Taipei is governed by the Personal Data Protection Act (PDPA) and its corresponding Enforcement Rules. Cybersecurity-related matters are regulated under the Cyber Security Management Act (CSMA). The Protection of Children and Youths Welfare and Rights Act of 1992 provides regulations for the protection of children and adolescents, including provisions related to internet use and personal data. Additionally, under the Chinese Taipei Civil Code, the consent of children and adolescents aged 7 or older but under 18 is not considered legally valid unless it is accompanied by the consent of a parent or guardian with legal responsibility.

19. Thailand

Thailand's Constitution establishes the State's responsibility to safeguard children's welfare, dignity, and development, and reflects international principles such as the UN Convention on the Rights of the Child. Building on this foundation, the Child Protection Act B.E. 2546 (2003) serves as the economy's primary child protection statute. It defines a child as a person under eighteen and provides mechanisms to prevent abuse, exploitation, and neglect through local and provincial Child Protection Committees, intervention powers for child protection officers, welfare and rehabilitation services, and criminal sanctions for harmful conduct against children.

In the digital sphere, the Personal Data Protection Act B.E. 2562 (2019) (PDPA) offers the main legal protection for minors' personal data. The PDPA requires parental consent for processing the personal data of children under ten, and joint consent from both the minor and a legal representative for those aged ten to under twenty, unless full legal capacity is recognized. It mandates clear notices, lawful processing, guardian verification, and adequate security safeguards. Together, the Constitution, the Child Protection Act, and the PDPA form Thailand's core legal framework for ensuring the safety, welfare, and digital privacy of children and adolescents.

20. United States

In the United States, there is no comprehensive federal privacy law. Certain federal, state, and local laws address privacy in the United States. However, the Children's Online Privacy Protection Act (COPPA or the Act) is a federal law that applies to personal data collected online from children.

There are also sector-specific federal laws relating to the privacy of children, especially in relation to gaming, child pornography, and internet presence. Below are relevant federal privacy statutes:

1) Children's Online Privacy Protection Act (15 U.S.C. §§ 6501–6506); 16 C.F.R. 312

COPPA is a federal law that requires operators of certain websites and online services, or those with actual knowledge that they're collecting personal information online from a child under 13 years of age, to notify parents and obtain verifiable parental consent prior to collecting, using or disclosing personal data of any child under the age of 13. The Act also requires companies to enable parents to review and delete data collected from children under 13 years old. It requires companies to secure and dispose of the data when no longer needed and includes data minimization requirements as well. COPPA is enforced by the United States Federal Trade Commission (FTC) and can also be enforced by individual States. Under COPPA "the term 'child' means an individual under the age of 13." 15 U.S.C. §§ 6501 (1).

2) Family Educational Rights and Privacy Act, 20 U.S.C.§1232g

The FERPA requires educational agencies or institutions receiving federal funds to obtain student or parental, if the student is a minor, consent to disclose personally identifiable information in education records, protecting the privacy of student education documents. The FERPA applies to all schools that receive funds under an applicable program of the United States Department of Education and if the privacy requirements are unmet, funding can be withheld. Students must be allowed upon request, to access their records and students have the right to be provided an opportunity to correct or delete inaccurate, misleading or otherwise inappropriate data in their education records.

3) 18 U.S.C. § 2252

These provisions address data privacy in relation to child pornography, criminalizing the creation, possession, and distribution of images or videos containing sexually explicit depictions of children and adolescents.

4) Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (Take it Down Act), Pub. L. 119-12

The TAKE IT DOWN Act criminalizes the publication of nonconsensual intimate visual depictions. It also requires covered platforms to: (1) create a process for consumers to notify covered platforms of a nonconsensual intimate visual depiction on the platform; and (2) remove such depictions within 48 hours of receiving notice. The FTC is charged with enforcing this notice and removal process.

5) Privacy Rights for California Minors in the Digital World, SB 568 (California-specific privacy laws)

[Note: This is a California state law, not a comprehensive federal law applicable throughout the United States]

Commonly called the “Eraser Button” law, this law gives children and adolescents (individuals under 18) the right to remove or request removal of content they have posted on a website, mobile application, or online service. It also requires operators of such services to provide clear instructions and tools for content removal. This California law prohibits online operators (of websites or services) directed to children and adolescents from marketing/advertising products or services that children and adolescents are legally prohibited from buying. The law also legally bars the advertisement of certain products based on a minor’s personal data as well as allowing a third party to do so using such personal data of a minor. Similarly, the CalOPPA (California Online Privacy Protection Act) also requires services to post a conspicuous privacy policy explaining data collection and use. Furthermore, certain state privacy laws such as the CCPA (California Consumer Protection Act) require that a business obtain explicit consent prior to selling any personal data about an individual the business has actual knowledge is under 16 years old.

5) Delaware Online Privacy and Protection Act, Title 6, Chapter 12C (Delaware-specific privacy laws)

[Note: This is a Delaware state law, not a comprehensive federal law applicable throughout the United States]

Delaware also specifically prohibits operators of online services, including mobile applications, directed at children from advertising certain products inappropriate for children. It also requires operators to let users know what information is collected, how it's used, and how it's shared with third parties. Furthermore, like California, the law also prohibits an operator who has actual knowledge that a child is using its service from using the child's data to market certain products inappropriate for children or disclosing the data for the purpose of such marketing.

21. Viet Nam

The Law on Children (2016) is a key sectoral legislation that provides specific provisions regarding children's privacy rights (Article 21 on the right to privacy) and the responsibility to protect children in the online environment (Article 54).

In addition, Decree No. 13/2023/ND-CP on Personal Data Protection establishes general regulations on the protection of personal data, under which children's data is also governed.

Furthermore, Decree No. 72/2013/ND-CP on the management, provision, and use of internet services and online information includes provisions related to electronic games categorized by players' age groups, among other matters.

III. Comparative Analysis and Implications

Table 1 Overall legal framework governing protection of child and adolescents

APEC Economy	Special Law for Children/Adolescents (O/X)	Parental Consent Requirement	Special Online Protections
Australia	△ (Code being developed)	Yes (OAIC Children's Code in development)	Yes (Code under development)
Brunei Darussalam	X	No	No
Canada	X	General guidance only	Guidance only
Chile	X	No	Not specified
People's Republic of China	△ (In general laws, plus minor-specific rules)	Yes (under 14, written consent)	Yes (MPL & regulations)
Hong Kong, China	X	No specific law	Yes (Cap. 579, 390)
Indonesia	O (GR 17/2025)	Yes (in GR 17/2025)	Yes (GR 17/2025)

Japan	△ (Only sectoral laws)	Guidance only	Yes (Dating ban, apps limits)
Republic of Korea	X (Integrated in general laws)	Yes (under 14)	Yes (Network Act, Location Act)
Malaysia	△ (Consent rules)	Yes (under 18)	Yes (MCMC, ISP rules)
Mexico	△ (Best interest principle)	Yes (under best interest principle)	Not comprehensive
New Zealand	△ (Extra protection under general law)	No explicit provision	Yes (info access and breach handling)
Papua New Guinea	△ (Draft policies only)	No law yet	Draft policy proposed
Peru	△ (General law applies to all)	General principles apply	Yes (new decrees)
The Republic of the Philippines	O (Multiple sectoral laws)	Yes (across multiple acts)	Yes (OSAEC Act, ISP obligations)
The Russian Federation	△ (Content classification law)	Not specified	Yes (content harm law)
Singapore	) Supplemented its general law framework with regulatory guidance tailored to children's personal data, which is considered sensitive data under the PDPA.	Yes (under 13)	Yes (Code of Practices for Online Safety (Social Media Services, App Distribution Services)
Chinese Taipei	△ (Civil Code + Welfare Law)	Yes (Civil Code 7–17)	Yes (Youth Welfare Act)
Thailand	O	Yes (under 10)	No
United States	O (COPPA & state laws)	Yes (under 13)	Yes (COPPA, FERPA, state laws)
Viet Nam	O (Law on Children + Decrees)	Yes	Yes (Decrees, Internet law)

The legal system for children and adolescents varies greatly depending on each economy's political, economic, social, religious, and cultural situations and context. Especially, the disparity in age thresholds (13 vs 14 vs 16 vs 18) and consent mechanisms creates a complex compliance environment for digital service providers operating across the Asia-Pacific. A platform compliant in the United States (age 13) may be non-compliant in Korea (age 14) or Thailand. This regulatory fragmentation increases costs for businesses and may discourage the rollout of child-safe features in certain markets.

Given the borderless nature of the digital economy, the current patchwork of laws creates gaps where children in economies with nascent frameworks (e.g., Brunei Darussalam; Papua New Guinea) may receive lower levels of protection than their peers in economies with mature regimes (e.g., Australia; Japan; Korea).

The comparative analysis confirms that while APEC economies share a commitment to child protection, the means of achieving it are highly heterogeneous. There is a pressing need to move beyond disparate local approaches toward regional interoperability. Future policy initiatives should focus on harmonizing age verification standards, sharing technical best practices for "privacy-preserving" age assurance, and developing a common set of principles that bridge the gap between data privacy regulations and online safety laws.

Section 2 Distinction Between Adults and Children and adolescents in Personal Data Laws: Key Categories and Regulations

I. Introduction

As digital engagement among children and adolescents continues to expand, questions of how personal data laws account for age-based differences have gained prominence. Recognizing that children and adolescents may lack the cognitive maturity or legal capacity to fully comprehend the implications of data processing, many jurisdictions have introduced special safeguards or consent mechanisms for younger individuals. This section of the survey seeks to explore whether APEC member economies legally distinguish between adults and children and adolescents in the context of personal data, and if so, whether additional subcategories—such as children versus adolescents—are defined. Furthermore, it investigates whether distinct legal obligations, rights, or protective measures apply based on such age classifications. By identifying these distinctions, the survey aims to provide a comparative understanding of how legal systems tailor data protection frameworks to reflect the unique vulnerabilities and developmental needs of younger populations.

II. Status of APEC economies

1. Australia

The Privacy Act does not distinguish between adults and children and adolescents in the context of personal data.

Once developed, however, the Children’s Online Privacy Code, which is subordinate to the Privacy Act, will set out how the obligations in the Privacy Act must be complied with by social media and other online services likely to be accessed by children. This code may also include additional requirements that aren’t inconsistent with existing obligations.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

PIPEDA does not explicitly distinguish between adults and children and adolescents in the context of personal data. Instead, the law requires that any individual, regardless of age, must be able to provide meaningful consent for the collection, use, or disclosure of their personal data.

This means the individual must fully understand the nature, purpose, and consequences of the data processing at the time consent is sought. For children or adolescents, organizations are expected to assess whether the young person has the capacity to provide such informed and meaningful consent; if not, consent should be obtained from a parent or guardian. The focus is therefore on the individual's ability to comprehend and agree, rather than on a specific age threshold.

The Privacy Commissioner/Office of Privacy Commissioner (OPC), which enforces PIPEDA, has issued guidance specifying that for children and adolescents, the ability to provide meaningful consent depends on the child's maturity and capacity to understand what is being consented to. As a general (non-binding) guideline, organizations are encouraged to obtain parental consent for children under the age of 13.

However, this is guidance and not a statutory requirement.

4. Chile

According to the personal data protection law, the processing of personal data of children (under the age of 14) must be based on the best interests of the child, and the consent of a parent or legal guardian is mandatory.
For adolescents (aged 14 to under 18), their personal data is treated similarly to that of adults, but the best interests standard still applies. In the case of processing sensitive personal data of adolescents, the consent of a parent or legal guardian is also required.[1]

5. People's Republic of China

Article 31 of the Personal Information Protection Law (PIPL), Article 72 of the Law on Protection of Minors and Article 2 of the Provisions on the Protection of Children's Personal Information in Cyberspace of the People's Republic of China set the age threshold for the capacity to give consent at 14 years.
Accordingly, minors aged 14 and above are considered sufficiently mature data subjects capable of understanding the significance and consequences of personal data processing and are therefore deemed able to provide independent consent.

6. Hong Kong, China

[1] https://fpf.org/blog/chiles-new-data-protection-law-context-overview-and-key-takeaways/

There is no distinction.

7. Indonesia

GR 17/2025 defines a “child” as an individual under the age of 18.
While the regulation does not further subdivide younger children and adolescents into additional categories, it allows a 17-year-old adolescent to provide direct consent for the processing of their personal data. However, electronic system operators (ESOs) must immediately notify the parent or guardian and provide a six-hour window during which they may object. If no objection is raised within that time, the adolescent’s consent is considered valid.
For children under the age of 17, stricter rules apply. ESOs are required to actively seek consent from a parent or guardian within 24 hours, and the child must be prevented from using the service until such consent is obtained. During this 24-hour period, the child is not allowed to access the service.

8. Japan

Under the APPI, there are no provisions that apply exclusively to the handling of personal data belonging to children and adolescents.

However, the APPI guidelines state that when obtaining consent from the individual as required under the APPI for the collection of personal data, if the minor is deemed not to have the capacity to understand the consequences of consenting to the handling of their personal data, consent must be obtained from a legal guardian or equivalent party.

9. Republic of Korea

The PIPA does not distinguish between adults and children and adolescents as data subjects. Instead, it specifically regulates cases where the data subject is a child under 14 years of age. If the data subject is under 14 years old:

- Consent from their legal guardian must be obtained (Article 22-2, Paragraph 1).
- When providing notifications, easy-to-understand formats and simple language must be used (Article 22-2, Paragraph 3).
- The legal guardian of a child under 14 years of age can exercise the child's rights, such as requesting access, with the data controller (Article 38, Paragraph 2).

On the other hand, the Location Information Act specifically regulates children under 14 years of age and children aged 8 or younger among location data subjects:

- To collect, use, or provide the personal location data of a child between the ages of 8 and under 14, consent from their legal guardian must be obtained, and it must be confirmed that the legal guardian has consented (Article 25, Paragraph 1).

If a guardian responsible for protection consents to the collection, use, or provision of personal location data of a child aged 8 or younger for the protection of the child's life or body, it is considered as if the child has consented (Article 26).

10. Malaysia

Under Act 709, the definition of "data subject" refers to "an individual who is the subject of the personal data." In this context, there is no distinction between adults and children and adolescents regarding personal data protection, as the law treats all individuals (data subjects) the same regardless of age. However, Act 709 requires that parental consent be obtained for the processing of children and adolescents' personal data under the age of 18.

11. Mexico

The only distinction made by the laws on personal data protection between adults and children and adolescents is the one indicated in the previous point, so there is no subdivision between children and adolescents, and other categories.

12. New Zealand

The New Zealand Privacy Act does not distinguish between adults and children and adolescents except in the circumstances described in 1.1.

Other New Zealand laws do define the age of children and young people:

1. The Oranga Tamariki Act 1989 defined a child as an individual under the age of 14, and a young person as an individual of and over the age of 14 but under the age of 18 years.

2. The Children’s Act 2014 defines a child as a person under the age of 18 years, a person who is under the age of 21 years and has been in state care, or a person who is under the age of 25 and receiving transition support from Oranga Tamariki

3. The Health Act 1956 provides that a parent or guardian is a representative for the purposes of making an access request where the child is under the age of 16.

13. Papua New Guinea

There is no distinction under official legislation.

14. Peru

Peruvian law distinguishes between adults and children and adolescents in matters of consent. For children and adolescents under the age of 14, personal data cannot be processed without the explicit consent of a parent. However, for children and adolescents over the age of 14 but under 18, consent may be granted based on the individual's capacity. In such cases, the relevant information must be provided in a manner that the minor can understand and in compliance with regulatory requirements.[2]

15. The Republic of the Philippines

The Philippines' Data Privacy Act (DPA) does not explicitly distinguish adults and minors. However, the Civil law definition of the age of majority is also applicable. This is reflected in the Advisory on Guidelines on Child-Oriented Transparency:

'child' refers to a person below eighteen (18) years of age or those eighteen (18) or over but are unable to fully take care of themselves or protect themselves from abuse, neglect, cruelty, exploitation, or discrimination because of a physical or mental disability or condition;

As to whether children and adolescents are subdivided into more specific categories, the following laws provide for such categorization, but not specifically in the context of personal data:

• Juvenile Justice and Welfare Act, provides that children below 15 years old are exempt from criminal liability; while those from 15 to below 18 years old may be held liable if they acted with discernment

• Republic Act No. 9231, the Anti-Child Labor Law, provides that children below 15 years of age are generally prohibited from working except under strict conditions; those from 15 to below 18 years old should have regulated working hours and prohibited from hazardous occupations.

16. The Russian Federation

---

[2] Reglamento De La Ley Nº 29733, Ley De ProtecciÕn De Datos Personales (Regulation of Law No. 29733, the Personal Data Protection Law)

Chapter IV, Article 22(2)

Individuals over fourteen (14) and under eighteen (18) years of age may, in accordance with their capacity, give consent to the processing of their personal data, provided that the information supplied has been expressed in language understandable to them, pursuant to the applicable regulations.

There are no specific laws in the content, gaming, or education sectors that directly regulate children's personal data.

17. Singapore

Under the PDPA, the validity of a minor's consent depends on the individual's understanding on the nature and implications of that consent. The PDPC's Children Advisory Guidelines indicates that older minors (e.g. around age of 13 and above) may be considered capable of providing consent, while parental or guardian consent should be obtained where the minor lacks in such capacity.[3]

18. Chinese Taipei

The PDPA does not distinguish between adults and children and adolescents in its provisions. However, under the Chinese Taipei Civil Code, the consent of children and adolescents between the ages of 7 and 18 is not legally valid unless it is accompanied by the consent of a parent or guardian with legal responsibility. [4] For children under the age of 7, only the person with parental responsibility may provide valid consent. According to Article 13 of the Chinese Taipei Civil Code, children and adolescents under the age of 7 have no legal capacity to act, while those aged 7 to under 18 are considered to have limited legal capacity. [5]

19. Thailand

Under Thailand's Personal Data Protection Act (PDPA), a minor is defined in line with the Civil and Commercial Code as any person under 20 years of age, unless the individual has obtained full legal capacity through marriage. Within this broad category of minors, the PDPA distinguishes younger children from older minors for the purpose of data-processing consent. A child is effectively treated as a minor under the age of ten, and for this group the law requires that consent for the collection or use of personal data must be provided exclusively by a parent or legal guardian, as the child's own consent has no legal effect. For minors aged ten to under twenty, the PDPA adopts a combined-consent model in which both the minor and the parent or legal guardian must give consent, unless the minor has full legal capacity for a particular legal act under civil law. Through this structure, the PDPA establishes a tiered protection regime that imposes the strictest safeguards on children

[3] cipl childrens privacy policy paper i - international issues compliance challenges 21 oct 2022 .pdf

[4] https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/asia-pacific/taiwan/topics/legal-bases-for-processing-of-personal-data

[5] https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=B0000001

under ten while requiring shared responsibility for older minors who have greater, but still limited, legal capacity.

20. United States

COPPA sets the age of consent for purposes of data privacy at 13. Under the age of 13 years old, consent must be given by the holder of parental responsibility for the child according to COPPA. Companies are obligated to verify such consent using a method set forth in the COPPA Rule or another method that is "reasonably calculated, in light of available technology, to ensure that the person providing consent" holds parental responsibility for the child 16 C.F.R. §§ 312.2, 312.5(b)(1).

It should be noted that COPPA does not apply to children ranging from ages 13-17 years old (teenagers). There is no federal law equivalent for teenagers' data privacy. The Federal Trade Commission has challenged companies' practices with respect to collecting, using or disclosing consumers' personal data online (some cases likely included teens' data) were unfair or deceptive in violation of the Federal Trade Commission Act.

On a narrower scale, sector-specific laws tend to distinguish children and adolescents based on the age of 18, depending on the context. The FERPA and 18 U.S.C. § 2256 defines the age of consent as 18 and older for the purposes of privacy in educational records and child pornography (respectively).

21. Viet Nam

Currently, Government Decree No. 13/2020 includes provisions on the processing of children's personal data (Article 20). The Draft Law on Personal Data Protection also contains provisions under Article 20 regarding the protection of children's personal data. At present, neither the aforementioned decrees nor the draft law provides a clear classification between young children and adolescents.

III. Comparative Analysis and Implications

Table 2 Distinction Between Adults and Children and Adolescents in Personal Data Laws

APEC Economy	Age Distinction (Y/N)	Parental Consent Required	Age of Independent Consent
Australia	N	Code in development	Not defined yet
Brunei Darussalam	N/A	No info	N/A
Canada	Y (based on maturity)	Yes if under 13 or lacks capacity	Maturity-based

Chile	Y (14 cut-off)	Yes (<14); case-by-case (14–18)	14+
People's Republic of China	Y (8/14/18 distinction)	Yes <8 always; 8–14 if not mature	14+ generally (8–14 limited)
Hong Kong, China	N	N/A	N/A
Indonesia	Y (17/under 17)	Yes <17, notice system for 17	17 (with parental veto)
Japan	Y (case-by-case)	Yes if no capacity	If capable
Republic of Korea	Y (under 14)	Yes <14	Not allowed <14
Malaysia	Y (under 18)	Yes <18	<18 not allowed
Mexico	N (general rule only)	Yes (underage)	Not specified
New Zealand	Y (varies by law)	Yes <16 (only under the Health Act 1956)	Varies (14/16/18)
Papua New Guinea	N	N/A	N/A
Peru	Y (14/18)	Yes <18	14–17 if capable
The Republic of the Philippines	N (civil law applies)	Yes (DPA + civil def.)	Not explicit
The Russian Federation	N	Not specified	N/A
Singapore	Y (under 21/13+)	Yes <13 (practice); <21 legal)	13+ (common practice)
Chinese Taipei	Y (7/18, Civil Code)	Yes <18	7–18 limited, <7 none
Thailand	Y (under 10)	Yes<10	10+
United States	Y (under 13 COPPA)	Yes <13 (COPPA)	13 (COPPA)
Viet Nam	Y (general rule)	Yes (per decree)	Not clearly defined

There are many laws that require parental consent under personal data protection laws, but the age criteria are different. For businesses that provide the same service in multiple APEC economies, it can be difficult to comply with the regulations of all APEC economies at the same time.

The disparity in age thresholds—10, 13, 14, 16, 18, 20/21—creates a significant compliance burden for digital service providers operating across the APEC region.

- A platform must build dynamic consent flows that trigger parental verification at age 13 in the United States, age 14 in Korea, and potentially age 18 or 20 in Southeast Asian economies.
- The requirement for "joint consent" (e.g., Thailand) or "limited capacity" validation (e.g., Chinese Taipei) adds technical complexity compared to simple "parental gate" models.

Strict requirements for parental consent up to high ages (e.g., 18 or 20) in some economies may inadvertently restrict adolescents' independent access to educational or social resources, infringing on their rights to participation and information. Conversely, low thresholds (e.g., 13) may leave vulnerable children and adolescents exposed to exploitative data practices.

The comparative analysis highlights that while the goal of protecting minors is shared, the method of defining "who is a minor" varies deeply based on cultural, civil, and common law traditions. Moving forward, APEC economies may benefit from harmonizing Age Bands by encouraging a regional consensus on "tiered" protections that distinguish between young children (needing strict parental control) and adolescents (needing safety-by-design and guided autonomy).

Section 3 Criteria and Scope of Personal Data Privacy Regulations for Children and Adolescents

I. Introduction

To assess the effectiveness and consistency of legal protections across APEC member economies, it is essential to understand the scope and basis for the application of privacy regulations to children and adolescents. Some jurisdictions apply child-related rules only to services explicitly targeting young users, while others apply enhanced protections to all platforms likely to be accessed by children, regardless of their primary target audience. Therefore, this section examines how each APEC economy defines the scope of its child and adolescent privacy regulations. This aims to clarify the regulatory environment and highlight the different approaches to regulating the processing of children and adolescents' personal information.

II. Status of APEC economies

1. Australia

The Privacy Act does not cover State or Territory public agencies. This includes State and Territory educational institutions.

The Privacy Act, however, applies to federal government agencies and private sector organizations with an annual turnover of over AUD 3 million. This includes private educational institutions where they:

- have an annual turnover of over AUD 3 million
- are connected to an organization with an annual turnover of more than AUD 3 million
- provide a health service, even if this is not their primary activity (i.e. keeping records of child’s medical condition or general health, or doing activities to maintain their health, such as making sure they take prescribed medication or providing first aid).

Once finalized, the Children's Online Privacy Code will apply to social media services likely to be accessed by children or other entities specified in the code.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

No information was found in relation to this issue.

4. Chile

The personal data protection regulations in Chile apply not only to data controllers or data processors established within Chile, but also to entities that offer services or products in Chile or process information on behalf of such entities.[6]

5. People's Republic of China

The Regulation on the Protection of Minors in Cyberspace stipulates that online product and service providers, personal information processors, and smart device manufacturers and sellers shall fulfill the obligation of protecting minors in cyberspace.

6. Hong Kong, China

All provisions in the PDPO (including the data protection principles therein) are applicable to the personal data of children and adolescents.

7. Indonesia

GR 17/2025 applies broadly to all electronic system operators (ESOs) in Indonesia—whether public or private, domestic or foreign—that are intended to be used or accessed by children (defined as individuals under the age of 18). This includes platforms such as social media, online games, e-commerce, educational apps, smart toys and devices, and

[6] https://fpf.org/blog/chiles-new-data-protection-law-context-overview-and-key-takeaways/

streaming services.
Moreover, even if a platform is not explicitly designed for children, it may still fall under the regulation if it is reasonably likely that children will use it. To make such determinations, the government considers several indicators—for example, whether the platform's rules (public or internal) suggest it is child-oriented, whether there is strong evidence that a high percentage of regular users are children, whether advertisements are targeted at children, whether the design and visual elements appeal to children, or whether the platform closely resembles others known to be popular among children.
However, the specific criteria for these indicators remain unclear. For instance, the term "strong evidence" has not been precisely defined. The Ministry of Communications and Digital Affairs is expected to provide detailed guidance on these matters through a forthcoming ministerial regulation.

8. Japan

No information was found in relation to this issue.

9. Republic of Korea

Provisions in the PIPA concerning the protection of children's personal data apply to all data controllers. This means that relevant obligations aren't imposed only on specific types of data controllers.

While there are no explicit regulations in other laws, the Personal data Protection Commission ("PIPC") takes the position that, by comprehensively considering the content and delivery method of a service, it should be assessed whether children or adolescents can reasonably be expected to use it. For businesses where such use is indeed anticipated, the PIPC recommends collecting age information to identify if a user is a child before providing the service, as explained in Section 3.3.

The types of services that the PIPC provides as examples, which can be expected to be used by children or adolescents, include:

- Services where the content and delivery method are visually or audibly targeted at children.
- Apps or websites where models or characters are child oriented.

Services (such as SNS, messengers, games, portals, or learning platforms) that the majority of children or adolescents can access and use.

10. Malaysia

Under Act 709, the processing of children and adolescents' personal data in commercial transactions requires parental consent. The data must only be used for the specific purpose for which it was collected, ensuring that the privacy of children and adolescents is protected.

11. Mexico

The fundamental criteria for the application of data protection legislation concerning children and adolescents is to prioritize the best interests of the child, in accordance with the applicable legal provisions.

This means that when processing their personal data, special measures must be adopted to ensure enhanced protection, considering their increased vulnerability.

In the secondary legislation applicable to the public sector in Mexico, when a minor is involved in a review process, conciliation is generally not allowed if any of the minor's rights have been violated. The only exception is when the minor has properly accredited legal representation. This rule aims to ensure the protection of the rights of children and adolescents during such procedures.

12. New Zealand

The New Zealand Privacy Act does not distinguish between adults and children and adolescents except in the circumstances described in 1.1.

Other New Zealand laws do define the age of a children and young people:

1. The Oranga Tamariki Act 1989 defined a child as an individual under the age of 14, and a young person as an individual of and over the age of 14 but under the age of 18 years.

2. The Children's Act 2014 defines a child as a person under the age of 18 years, a person who is under the age of 21 years and has been in state care, or a person who is under the age of 25 and receiving transition support from Oranga Tamariki

3. The Health Act 1956 provides that a parent or guardian is a representative for the purposes of making an access request where the child is under the age of 16.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

The PDPL and its accompanying regulations apply not only to database owners and data controllers located in Peru, but also to any entities engaged in personal data-related activities within Peruvian territory.[7]

15. The Republic of the Philippines

The Data Privacy Act of 2012 and the Advisory on Children applies to all entities that are engaged in the processing of children's personal data, whether in a digital or physical environment. The Advisory specifically covers products or services specifically intended for children or likely to be accessed by children.

16. The Russian Federation

According to the Russian Civil Code and Federal Law No. 152-FZ, individuals under the age of 18 are considered to have limited legal capacity. As a general rule, the authority to provide consent rests with a parent, guardian, or other legal representative. However, in certain cases, children from the age of 14 are allowed to act independently to some extent—for example, when engaging in small-value transactions.

17. Singapore

The *Advisory Guidelines on the PDPA for Children's Personal Data in a Digital Environment* specify certain types of businesses that are required to exercise particular caution when handling children's personal data. These include social media platforms, educational technology providers, online gaming services, and smart toy manufacturers, among others.[8]

18. Chinese Taipei

All entities that process[9] personal data and determine the purposes and means of such processing. [10]

---

[7] https://insightplus.bakermckenzie.com/bm/data-technology/peru-new-regulations-of-the-personal-data-protection-law_1

[8] https://www.eversheds-sutherland.com/en/finland/insights/childrens-data-new-guidelines-issued-by-the-singapore-personal-data-protection-commission

[9] https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021

[10] https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/asia-pacific/taiwan/topics/key-definitions

19. Thailand

Thailand's Personal Data Protection Act applies to all data controllers, both online and offline, including provisions regarding the protection of personal data of minors.

20. United States

COPPA applies to any commercial website, online service, or app directed to children under 13 and in instances where the operator of a website, service, or app has actual knowledge that a user is under 13. The determination whether a site is child-directed depends on content, design, marketing, and audience.

The FERPA applies to all educational institutions that receive funds from the United States government, which includes both public and private schools.

21. Viet Nam

According to the Law on Children (2016), the criteria for applying privacy-related provisions to children are defined as individuals under the age of 16.

Some applicable services include:

Electronic games and mobile applications: regulated under Decree No. 72/2013/ND-CP on the management, provision, and use of internet services and online information;

Social networks and digital platforms: governed by the Law on Cybersecurity (2018) and Decree No. 13/ND-CP on Personal Data Protection.

III. Comparative Analysis and Implications

Table 3 Criteria and Scope of Personal Data Privacy Regulations for Children and Adolescents

APEC Economy	Scope of Application
Australia	Federal agencies & private orgs >AUD 3 million; excludes state entities
Brunei Darussalam	No info
Canada	No info
Chile	Covers local/foreign offering services in Chile

People's Republic of China	Applies to cyberspace sector
Hong Kong, China	PDPO applies to all, including children
Indonesia	All ESOs, including foreign platforms used by children
Japan	No info
Republic of Korea	All data controllers; PIPC gives guidance on child-expected services
Malaysia	Act 709 applies to commercial transactions involving children and adolescents
Mexico	Focus on best interest; public sector limited conciliation rules
New Zealand	Privacy Act applies to all; Health Act applies for access if <16
Papua New Guinea	No info
Peru	Applies to any data handling within Peru
The Republic of the Philippines	Applies to all processors targeting or accessible to children
The Russian Federation	General civil law + limited child transactions age 14+
Singapore	Applies to all private sector organizations. PDPC's regulatory guidance includes examples from child-relevant digital services (e.g. edtech, gaming).
Chinese Taipei	All entities determining purposes/methods
Thailand	No info
United States	COPPA for child-directed online services; FERPA for certain educational institutions
Viet Nam	Children defined <16; law applies to such services

The standards for applying personal data regulations related to children and adolescents are very different in each APEC economy. For businesses providing services in multiple APEC economies, it can be very burdensome and difficult to confirm whether the individual is a perpetrator.

The shift toward the "likely to be accessed" standard (seen in Australia; Indonesia; Korea) challenges the business model of "general audience" platforms. Platforms that previously claimed to be "for adults" (but had many child users) will increasingly be forced to implement age assurance measures for *all* users to distinguish minors. This raises privacy concerns for adult users and technical costs for businesses. Conversely, in "actual knowledge" jurisdictions (United States), platforms may be incentivized to *avoid* gaining knowledge of child users to escape liability, potentially leaving children unprotected on popular mixed-audience sites. Also, businesses face legal uncertainty without clear regulatory guidance (as noted in the Indonesia section).

The scope of application is a critical battleground in child privacy. The trend in the APEC region is moving away from narrow "directed to children" definitions toward a broader "likely to be accessed" standard. This evolution reflects a recognition that children are active participants in the general digital ecosystem, not just in walled gardens.

Section 4 Enforcement and Sanctioning Trends for Children and Adolescents' Personal Data Processing

I. Introduction

As the misuse or mishandling of children and adolescents' personal data can result in more severe and lasting harm than comparable violations involving adults, many jurisdictions have adopted strengthened enforcement approaches or imposed heightened penalties when minors are affected. This section examines whether APEC economies differentiate sanctions or enforcement mechanisms in cases involving children and adolescents, and whether stricter practical responses—such as higher fines, enhanced administrative actions, proactive monitoring, or accelerated takedown requirements—are applied even when the legal standards formally remain the same. By reviewing both statutory provisions and real-world enforcement practices, this section seeks to identify emerging trends in how regulators prioritize the protection of children and adolescents and tailor sanctions to reflect their heightened vulnerability in the digital environment.

II. Status of APEC economies

1. Australia

Under section 13G of the Privacy Act the privacy regulator, the OAIC, is able to seek civil penalties for cases of 'serious or 'repeated' interferences with privacy.

There are certain factors which may be relevant when considering whether an interference is 'serious', including the consequences of the interference (depending on the circumstances, the consequences of the interference may be more serious for children or adolescents) and whether the affected individual/s are disadvantaged or vulnerable.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

Under PIPEDA, there are no different statutory penalties or legal enforcement mechanisms for cases involving the personal data of children or adolescents compared to general cases.

The law applies equally to all individuals, regardless of age—there are no elevated fines, additional enforcement tiers, or formal distinctions based on whether the data subject is a minor.

However, in practice, the OPC often treats cases involving children's or adolescents' personal data with greater regulatory seriousness. This does not change the legal standards or maximum fines, but it does result in practical differences in enforcement.

4. Chile

Following the implementation of the new personal data protection law in 2026, the processing of children's and adolescents' personal data is expected to be subject to significantly different levels of sanctions compared to general cases.

5. People's Republic of China

No specific legal basis was found indicating that sanctions related to the processing of children's and adolescents' personal data differ from general sanction levels.

6. Hong Kong, China

There is no such difference.

7. Indonesia

The Ministry of Communications and Digital Affairs holds supervisory authority over the implementation of electronic systems related to child protection. This includes monitoring compliance, receiving and investigating reports and complaints, conducting preliminary and follow-up investigations, and accessing the systems, data, and documents of electronic system providers (ESPs). The Ministry also has the authority to summon ESPs, request explanations, inspect digital infrastructure, and cooperate with other government agencies and experts.
Violations of GR 17/2025 may result in administrative sanctions, including:

- Issuance of warning letters
- Imposition of administrative fines
- Temporary suspension of products, services, or functionalities
- Blocking of system access

Administrative sanctions imposed on ESPs may be publicly disclosed through official channels.

In addition, if a failure to protect children’s personal data is identified, further administrative sanctions may be imposed under the Personal Data Protection Law (Law No. 27 of 2022).

8. Japan

Under the APPI, even if personal data of children or adolescents are leaked, there is no clear difference in the legal level of penalties or sanctions compared to cases involving adults.

9. Republic of Korea

Regarding the processing of personal data of children or adolescents, neither the laws themselves establish different levels of sanctions compared to general personal data processing, nor do regulatory bodies practically treat the imposition or level of sanctions differently.

However, as obligations concerning the protection of a child's personal data (e.g., the obligation to obtain consent from a legal guardian) exist as separate provisions under the PIPA, acts that violate these legal obligations (i.e., processing the personal data of a child under 14 years of age without obtaining the legal guardian's consent) may be subject to an administrative fine of up to 3% of the total sales revenue (Article 64-2, Paragraph 1, Subparagraph 2) and/or imprisonment for up to 5 years or a fine not exceeding KRW 50 million (Article 71, Subparagraph 3).

10. Malaysia

Under Act 709, enforcement actions do not differ based on the age of the data subject, including children and adolescents under 18. The penalties, such as fines of up to MYR 500,000 or imprisonment for up to 3 years, apply equally to all violations. The focus of enforcement is on the type of violation, rather than the age of the data subject (individual) involved.

11. Mexico

One of the parameters to be considered when individualizing a sanction is the nature of the personal data involved. In cases related to children and adolescents, the authorities must impose a higher sanction.

Even if the legal standard is generally the same, in practice, there are stricter consequences when processing the personal data of children or adolescents.

According to Article 60 of the private sector data protection law, authorities must consider several factors when deciding on ruling a sanction, including the nature of the data, whether the violation is intentional, the company's economic capacity, recidivism, and whether the data controller clearly refused to respect the data subject's rights.

When the personal data belongs to a child or adolescent, it is considered a special category due to their vulnerability. This means a higher level of protection is required, and any violations usually result in more severe penalties.

Since the nature of the data is a key factor, authorities are expected to impose higher sanctions when the data involves children and adolescents.

12. New Zealand

No. There are no variations in penalties or enforcement mechanisms with respect to the access, use, and disclosure of children or young people's personal data.

However, personal data of children and young people is generally considered more sensitive than information about adults that may influence or impact an assessment of serious harm caused by a breach and thus any enforcement action taken as a result of that breach. It may also influence any damages awarded if the privacy interference was considered by the Human Rights Tribunal.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

In the case of children and adolescents, the level of sanctions for the collection and processing of personal data differs from that applied to adults. Consent must be given or approved by a parent or legal guardian responsible for the minor.
For children and adolescents aged 14 to 18, they may provide consent for the processing of their personal data themselves; however:

- The information provided must be presented in language that is understandable to children and adolescents, and
- This does not apply in cases where the law requires the involvement of a parent or legal guardian for support or authorization.

Additionally, personal data related to a minor's family members may not be collected directly from the minor. However, in applicable cases, it is permitted to collect information necessary to obtain consent—such as the name and address of the parent or guardian.[11]

15. The Republic of the Philippines

No information was found in relation to this issue.

16. The Russian Federation

No information was found in relation to this issue.

17. Singapore

Apart from the capacity to provide consent, there are no additional sanction provisions.

18. Chinese Taipei

- The personal data of children and adolescents under the age of 14 is classified as sensitive information. According to the Personal Data Protection Act, the collection, processing, and use of such sensitive data is prohibited except in the following six cases:
- When necessary to fulfill obligations under the law;
- When required by law;
- When the individual has voluntarily disclosed the information;
- For statistical or academic purposes;
- When disclosure serves the public interest.[12]

It has not been confirmed whether the personal data of children under the age of 14 is regulated as sensitive information.[13]

---

[11] https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/latin-america/peru/topics/legal-bases-for-processing-of-personal-data

[12] https://sandlineglobal.com/taiwans-data-privacy-law-overview/

[13] https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021

19. Thailand

Under Thailand's Personal Data Protection Act (PDPA), violations involving the personal data of children and adolescents are not subject to stronger or differentiated penalties compared to violations involving adults. Although the PDPA imposes stricter consent requirements for minors—such as requiring exclusive parental consent for children under ten and joint consent for older minors—the sanctioning provisions apply uniformly. This means that administrative fines, civil liability, and criminal penalties are the same regardless of whether the data subject is an adult or a minor. While regulators may treat incidents involving children more seriously in practice, the law itself does not provide for enhanced or aggravated penalties specifically for breaches affecting children or adolescents.

20. United States

COPPA applies civil penalties up to USD 53,088 (periodically adjusted) per violation or may result in significant settlements or consent decrees by the FTC. In practice, violations involving children are pursued more aggressively with higher fines and strict injunctive relief. One FTC matter involving children was Disney. In December 2025, the FTC announced that a federal judge has approved an order requiring Disney to pay USD 10 million to settle allegations that the company allowed personal data to be collected from children who viewed kid-directed videos on YouTube without notifying parents or obtaining their consent as required by the COPPA Rule.

21. Viet Nam

According to Decree No. 13/ND-CP, the processing of children's personal data requires the consent of the child if the child is 7 years of age or older, along with the consent of the parent or legal guardian as prescribed.

Entities authorized to process such data are required to verify the child's age prior to processing their personal data.

In certain cases, specified in Clause 3, Article 20 of Decree No. 13/2020, data controllers must cease processing and permanently delete or irreversibly destroy the personal data of children.

III. Comparative Analysis and Implications

Table 4 Enforcement and Sanctioning Trends for Children and Adolescents' Personal Data Processing

APEC Economy	Differentiated sanctions for violations of personal information protection regulations for children and adolescents

Australia	Civil penalties under OAIC; consequences for children considered in 'serious cases
Brunei Darussalam	No info
Canada	Same legal penalties; stricter practical enforcement
Chile	Stronger sanctions expected under 2026 law
People's Republic of China	No difference found
Hong Kong, China	No difference
Indonesia	Yes – fines, suspensions, blocking under GR 17/2025 + PDP Law
Japan	No difference
Republic of Korea	Separate provisions under PIPA; up to 3% revenue or 5 years prison
Malaysia	Same penalties apply regardless of age
Mexico	Higher sanctions for children and adolescents' data due to vulnerability
New Zealand	Same law; child data seen as more sensitive in practice
Papua New Guinea	No info
Peru	Stricter rules for children and adolescents; parental consent mandatory
The Republic of the Philippines	No info
The Russian Federation	No info
Singapore	No specific sanction difference
Chinese Taipei	Child data <14 = sensitive; stricter handling but unclear sanction difference
Thailand	No difference
United States	COPPA fines up to USD 53,088/violation; high enforcement priority
Viet Nam	Must delete data in some cases; age + parental consent required

The level of punishment for children and adolescents varies across APEC economies. The lack of explicit, harmonized "child-specific" penalty tiers in many economies may lead to under-enforcement in less mature jurisdictions. Without clear statutory mandates to impose higher fines, overworked regulators in developing economies may treat child data breaches as routine administrative errors rather than priority cases, leaving children in those regions less protected than their peers in Australia or the United States.

The reliance on regulator discretion creates uncertainty. APEC economies could benefit from cooperative discussions on how to calculate administrative fines for child data breaches.

While few APEC economies have distinct "child penalty laws" on the books, the operational reality is different. The "vulnerability" of the child is increasingly acting as a force multiplier for enforcement actions, leading to higher effective fines and more intrusive remedies. The future of enforcement lies not just in higher dollar amounts, but in the power to disrupt

business operations (data deletion, service blocking) to protect young users. To ensure legal certainty and robust protection, member economies should consider formalizing these "aggravating factors" into their respective statutory frameworks.

Chapter 3 Obligations for Privacy by Design (PbD) in Processing Children or Adolescents' Personal Data

In the field of personal data protection, preventive measures are generally more effective than reactive responses. Once a privacy breach occurs, the resulting harm—especially for children and adolescents—can be difficult or even impossible to remedy. As minors often lack the fully developed cognitive capacity to understand the meaning and consequences of data processing activities, a proactive and preventive approach is essential. In this context, the principle of *Privacy by Design* (PbD) has gained prominence.

PbD moves beyond ex post regulatory compliance and seeks to proactively manage risks by embedding privacy safeguards into the design of systems, services, and organizational operations from the outset. As such, PbD serves as a particularly critical protection mechanism in digital environments frequently accessed by children and adolescents.

This section examines how APEC member economies have adopted and implemented the PbD principle within their legal and regulatory frameworks.

Section 1. Privacy by Design Regulations for Children and Adolescents Services

I. Introduction

Children and adolescents, as data subjects with limited cognitive and decision-making capacity, require heightened protection when their personal data is processed. In recognition of this, regulatory and policy efforts across jurisdictions have increasingly emphasized the importance of integrating privacy protections from the early stages of service development. The concept of Privacy by Design (PbD) lies at the core of this proactive approach, promoting the identification and mitigation of privacy risks before they materialize.

This section analyzes whether APEC economies impose regulatory obligations requiring service providers to assess and prevent potential privacy risks at the planning and design stages of services involving children and adolescents. Additionally, where such requirements exist, it explores what specific factors must be considered in designing services that prioritize the privacy rights of younger users. Through this comparative review, the section aims to identify current regulatory trends, gaps, and best practices relevant to embedding child-focused privacy protections into digital service architectures.

II. Status of APEC economies

1. Australia

There are no laws in Australia that specifically address privacy protections for children or adolescents. However, under the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, federal agencies must conduct a *Privacy Impact Assessment* (PIA) for

projects deemed high-risk in terms of privacy. A project is considered high-risk if it introduces new or substantially modified methods of handling personal data that could have a significant effect on individuals' privacy. While the Code does not provide a fixed definition of what constitutes a "significant impact," agencies are encouraged to consider various factors—including whether vulnerable groups such as children or adolescents may face greater privacy risks—as part of their risk assessment process. In addition, the Office of the Australian Information Commissioner actively encourages through its website's Privacy Guidance for Organizations and Government Agencies, and the eSafety Commissioner promotes a Safety by Design framework initiative; however, this is not a mandatory requirement.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

In Canada, Privacy by Design (PbD) is not a legal requirement under the Personal data Protection and Electronic Documents Act (PIPEDA). Private-sector organizations are not formally obligated to conduct documented Privacy Impact Assessments (PIAs), and PbD is not mandated for any group, including children and adolescents.

4. Chile

Under Article 14 of Chile's Ley de Protección de la Vida Privada (LPPD), data controllers are subject to a legal obligation to implement protective measures starting from the design and default stages of any data processing activity. This includes the principle of protection by design and by default, requiring organizations to anticipate and mitigate privacy risks during the planning and development of services.

While the law does not contain child-specific provisions, its requirements extend to all data processing operations, including those involving children and adolescents. Data controllers are required to implement appropriate security measures to ensure the confidentiality, integrity, availability, and resilience of processing systems. This includes techniques such as pseudonymization and encryption of personal data, as well as conducting periodic audits to prevent unauthorized access, data loss, or manipulation.

5. People's Republic of China

No information was found in relation to this issue.

6. Hong Kong, China

As of now, Hong Kong, China does not have specific legal or regulatory requirements obligating service providers to assess or mitigate potential privacy risks from the planning or design stages of services involving children or adolescents. The existing legal framework, primarily governed by the Personal Data (Privacy) Ordinance (PDPO), outlines general data protection principles that apply uniformly across all age groups but does not impose heightened obligations for minors.

7. Indonesia

Under Government Regulation No. 17 of 2025 (GR 17/2025), Indonesia has adopted a privacy by default approach for electronic system operators (ESOs). This regulation mandates that ESOs implement the highest level of privacy protection automatically from the earliest stages of service design and development, without requiring user intervention.

GR 17/2025 also introduces child-specific provisions. Electronic service providers targeting children and adolescents are prohibited from using deceptive or non-transparent design features in the development or operation of their products, services, or functionalities.

Furthermore, the collection of precise geolocation data of children and adolescents is strictly prohibited, except where it is demonstrably necessary and limited in duration. The regulation also prohibits profiling of children and adolescents, unless it is clearly shown to serve the best interests of the child or is explicitly requested by the children or adolescents.

8. Japan

Under Japan's *Act on the Protection of Personal data* (APPI), there are no explicit legal provisions requiring service providers to assess or mitigate privacy risks to children or adolescents from the design or planning stages of a service. The APPI does not impose mandatory Privacy by Design or Privacy by Default obligations specific to minors.

However, the APPI's enforcement guidelines require all personal data-handling business operators to implement security measures that are necessary and appropriate to the level of risk—regardless of whether the personal data concerns children, adolescents, or adults. These measures must be determined with consideration of the potential severity of harm to an individual's rights and interests in the event of a personal data breach or similar incident.

9. Republic of Korea

As of now, there are no legal provisions in Korea that explicitly require service providers to implement Privacy by Design measures when processing the personal data of children and adolescents. Neither the Personal data Protection Act (PIPA) nor its subordinate regulations mandate that service providers assess or mitigate privacy risks from the design or planning stages specifically in the context of minors.

While PIPA imposes general obligations on personal data controllers to ensure the security and proper handling of personal data, these obligations apply uniformly and do not distinguish between adults and minors. As such, there are no specific Privacy by Design or Default requirements tailored to the unique vulnerabilities of children and adolescents.

10. Malaysia

Malaysia's Personal Data Protection Act 2010 (Act 709) does not explicitly mandate the implementation of Privacy by Design (PbD), including for services involving children or adolescents. However, the Act requires data controllers to adhere to seven core data protection principles—such as data minimization and purpose limitation—which promote proactive privacy management and are generally aligned with PbD principles, particularly when handling the data of minors.

In addition, the Department of Personal Data Protection of Malaysia is in the process of drafting comprehensive Guidelines on Data Protection by Design (DPbD). These forthcoming guidelines aim to instruct data controllers on how to integrate privacy protection into the design of both manual and digital systems, covering all aspects of personal data processing within an organization. Importantly, the DPbD guidelines are expected to include specific requirements regarding parental consent for processing the personal data of individuals under the age of 18, thereby introducing children- and adolescents-specific protections.

11. Mexico

Mexico's data protection laws for both the public and private sectors include mechanisms to assess and prevent privacy risks from the early stages of service design, including those involving children and adolescents.

In the public sector, Article 68 of the LGPDPPSO mandates a Privacy Impact Assessment (PIA) before implementing systems or policies involving significant personal data processing. In the private sector, Article 39(IX) of the LFPDPPP empowers the data protection authority to conduct privacy impact studies for new or significantly modified data processing operations.

Additionally, Privacy by Design and Privacy by Default are explicitly required under Article 24 of the LGPDPPSO. Both sectors must also conduct risk assessments to ensure data security across the processing lifecycle.

When designing services for minors, data controllers must consider the sensitivity of the data and the vulnerability of the data subjects. The best interests of the child, as defined in Article 4 of the Mexican Constitution and upheld by the Supreme Court, must guide all decisions involving children's and adolescents' data.

12. New Zealand

New Zealand does not have specific regulations requiring service providers to assess and prevent privacy risks from the design stage of services involving children or adolescents. However, all agencies—including service providers—must comply with the Information Privacy Principles (IPPs) under the Privacy Act 2020 when collecting, using, disclosing, or managing personal data. Especially, IPP 4 requires agencies to take extra care when collecting personal information about children.

There is no explicit requirement for a Privacy Impact Assessments (PIAs) to be completed when designing services that collect, use, store and disclose personal information about children and young people. While not legally mandated, guidance issued by the Privacy Commissioner encourages agencies to conduct Privacy Impact Assessments (PIAs) as a best practice. PIAs are recommended to help identify and mitigate privacy risks early in a project, thereby supporting compliance with the IPPs.

.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

Peru's data protection framework does not explicitly mandate the implementation of Privacy by Design in services that process the personal data of children or adolescents. However, data controllers are obligated to take appropriate measures to ensure data security, including preventing unauthorized access, loss, or destruction of personal data.

Recommended practices include adopting a risk-based approach to data protection, ensuring the encryption of personal data, and conducting regular assessments to identify vulnerabilities related to potential data breaches. Organizations are also expected to carry out periodic audits to demonstrate compliance with data protection standards.

While there are no specific legal provisions focused on children or adolescents, services involving minors must be designed in a way that respects the data subject rights established under Peru's data protection law.

15. The Republic of the Philippines

In the Philippines, service providers are legally required to assess and mitigate privacy risks from the early stages of service design, including when processing children's personal data. The National Privacy Commission (NPC) Circular on Security of Personal Data mandates a *Privacy Impact Assessment (PIA)* for all systems involving personal data. Additionally, the Advisory Guidelines on Child-Oriented Transparency recommend conducting a *Child Privacy Impact Assessment (CPIA)* before launching products or services that are intended for or likely to be accessed by children and adolescents.

The CPIA must consider a wide range of factors, including purpose and nature of processing, type and sources of personal data, system architecture (open/closed), data storage, disposal, and sharing methods, security measures, age range of users and expected impact, risk identification, involvement of parents or guardians, especially where high risk is present.

Organizations must implement appropriate measures to address risks identified through the PIA/CPIA, in line with the principle of the *best interests of the child* and *transparency*. Specific measures include Age Assurance Mechanisms (tools to determine users' age range, beyond self-declaration where risks are high. The mechanism must be lawful, privacy-compliant, and explained in a child-friendly manner) and Enhanced Privacy Controls that include Default high privacy settings (e.g., disabling geolocation, private profiles) and Accessible privacy settings that are easy for children and adolescents to understand and adjust.

16. The Russian Federation

Russia does not have a standalone law specifically dedicated to the protection of children's and adolescents' personal data. However, general data protection requirements are governed by Federal Law No. 152-FZ on Personal Data. While the law does not explicitly refer to Privacy by Design (PbD), Article 19 outlines mandatory measures for ensuring the security of personal data during processing, which reflect key PbD principles.

These measures include keeping records of personal data processing, detecting unauthorized access to personal data, restoring personal data that has been altered or destroyed, establishing access control rules for processed data.

Although there are no provisions in the law that specifically address age-based interface design, data minimization, or parental control, organizations are required to develop internal

policies that define data protection purposes and safeguards. This internal compliance obligation inherently supports a privacy-conscious design approach aligned with PbD principles.

17. Singapore

Singapore adopts a principles-based approach under the Personal Data Protection Act (PDPA) and does not mandate specific instruments such as the Privacy by Design or Privacy Impact Assessment obligations. However, organizations are expected to assess and manage risks, particularly where services may be accessed by children. PDPC's advisory guidelines further set out expectations when handling children's personal data and address key risks such as profiling and geolocation data.

This is particularly relevant when services may be accessed by or directed at children and adolescents.

18. Chinese Taipei

Chinese Taipei does not have explicit legal provisions that require service providers to assess or prevent potential privacy risks during the planning and design stages of services involving children or adolescents. There are no confirmed criteria specific to the protection of children's or adolescents' personal data, nor are there any mandatory Privacy by Design obligations in place.

However, under Chinese Taipei's Enforcement Rules of the Personal Data Protection Act, it is recommended that personal data processors, particularly those handling personally identifiable information, establish mechanisms for assessing the risks associated with data collection, processing, and use. Additionally, certain types of service providers may be required to conduct periodic audits depending on the sector in which they operate.

19. Thailand

No information was found in relation to this issue.

20. United States

In the United States, *Privacy by Design* (PbD) is not explicitly mandated at the federal level, but key laws and regulatory guidance incorporate PbD-aligned principles—particularly in the context of protecting children's and adolescents' personal data.

Under COPPA, operators of websites and online services directed to children under 13 or any operators with actual knowledge they are collecting or maintaining personal information from a child are required to implement "reasonable procedures to protect the confidentiality, security, and integrity" of personal data. While COPPA does not formally require PbD, staff at the Federal Trade Commission (FTC) has published information referencing Privacy by Design in its official guidance.

At the state level, laws such as California's California Privacy Rights Act (CPRA) include provisions that mirror PbD principles. These include mandates for reasonable security

procedures, data minimization, and greater accountability, although an explicit, formal requirement for PbD is not codified.

When designing services that involve children or adolescents, different United States guidance and regulations, such as California Age-Appropriate Design Code Act(CAADCA), emphasize various principles, such as collecting only what is strictly necessary for the service (Data minimization), clearly informing users (and parents) about what data is collected and how it is used (Transparency), implementing strong technical and organizational safeguards such as encryption, authentication, and staff training (Security) using built-in mechanisms to limit risk and protect data by default (Automated safeguards), ensuring interfaces and content are suitable for children's cognitive levels (Age-appropriate design), securing verifiable parental consent before collecting data from users under 13 (Parental consent and verification), avoiding targeting children with personalized advertising or profiling practices (Limitations on profiling and advertising).

21. Viet Nam

Viet Nam's legal framework incorporates core elements of Privacy by Design (PbD), particularly for online services involving the personal data of children, even though the term is not explicitly used. Under Clause 2, Article 54 of the Law on Children, providers of online information and communication services must implement measures to ensure the safety and privacy of children's personal data. This obligation is reinforced by Decree No. 13/2023/ND-CP on Personal Data Protection, which introduces risk-based requirements that align with PbD principles.

Specifically, Article 24 of the Decree requires organizations processing personal data to maintain a Personal Data Processing Impact Assessment Record, including identification of potential privacy risks and the measures adopted to mitigate them. Additionally, Article 25 mandates that risk assessments be carried out when transferring personal data abroad.

When designing services involving children, providers must establish mechanisms to obtain explicit and verifiable parental or guardian consent. Data collection must have a clearly defined and limited purpose, and the use of children's data for unrelated or inappropriate purposes—such as targeted behavioral advertising without consent—is prohibited. Transparency is required, with information presented in simple, age-appropriate language. Strong security measures, including encryption and access control, must be built into the system from the beginning. Services must also support parents or guardians in exercising children's data rights, such as access, correction, or deletion.

While Viet Nam does not formally mandate Privacy by Design, the current regulatory structure effectively requires early integration of privacy and safety considerations, particularly when handling children's personal data.

III. Comparative Analysis and Implications

Table 5 Privacy by Design Regulations for Children and Adolescents Services

	PbD Required	Key Points

Australia	No	PIA required for high-risk projects in federal agencies. Children may be considered in risk assessment.
Brunei Darussalam	N/A	No information was found in relation to this issue.
Canada	No	PbD not required under PIPEDA; no child-specific mandates but caution encouraged.
Chile	Yes	LPPD Article 14 mandates PbD. General application includes children and adolescents.
People's Republic of China	N/A	No information was found in relation to this issue.
Hong Kong, China	No	PDPO applies generally; no specific mandates for children or adolescents
Indonesia	Yes	GR 17/2025 mandates privacy by default; bans deceptive design, profiling, geolocation without necessity.
Japan	No	APPI requires risk-based security measures; no child-specific mandates.
Republic of Korea	No	No explicit PbD obligation under PIPA; obligations apply uniformly.
Malaysia	No (in progress)	Act 709 encourages PbD principles; Guidelines under development with child-specific consent provisions.
Mexico	Yes	PIA required in both sectors; PbD mandated; child protections guided by best interest principle.
New Zealand	No	PIA recommended by Privacy Commissioner, not mandated; no child-specific provisions with respect to service design.
Papua New Guinea	Unknown	No survey data available.
Peru	No	Security measures required; PbD not mandated but risk-based practices encouraged.
The Republic of the Philippines	Yes	PIA and CPIA required; guidelines mandate age assurance, parental consent, and high privacy settings.

The Russian Federation	No (but implicitly aligned with PbD principles)	Federal Law 152-FZ includes risk control and access management; internal policy required.
Singapore	No	No PbD mandate; PDPA Advisory Guidelines further set out expectations when handling children's personal data and address key risks of greater concern vis-à-vis children, such as profiling and geolocation data.
Chinese Taipei	No	No PbD mandate; risk assessment and audits recommended under enforcement rules.
Thailand	Unknown	No survey data available.
United States	No (recommended)	COPPA mandates reasonable procedures for security for under-13's data; FTC promotes PbD. CPRA mandates security and minimization.
Viet Nam	Yes	Law on Children and Decree 13 require risk assessments, parental consent, and child-appropriate design.

These findings suggest that, despite growing recognition of the heightened privacy risks faced by children and adolescents, Privacy by Design obligations remain fragmented and inconsistently operationalized across APEC economies. Jurisdictions that have adopted explicit PbD or child-specific impact assessment requirements tend to articulate clearer expectations regarding risk identification, default privacy settings, and age-appropriate service design. In contrast, economies relying primarily on general data protection principles leave substantial discretion to service providers, which may result in uneven levels of protection for children and adolescents, particularly in fast-evolving digital environments.

From a regulatory policy perspective, the absence of harmonized PbD standards for children and adolescents poses challenges for cross-border digital services operating within the APEC region. Divergent regulatory approaches increase compliance complexity for service providers while potentially undermining effective protection where services are designed to meet only the lowest common denominator. This fragmentation underscores the value of greater cooperation on child-centered privacy protections at the design stage, without imposing rigid or one-size-fits-all regulatory models.

Section 2. Practical Implementation of Privacy by Design for Children and Adolescents

I. Introduction

While legal mandates play a critical role in shaping data protection standards, the absence of binding regulations does not necessarily preclude the implementation of robust privacy safeguards, particularly for vulnerable groups such as children and adolescents. Across various jurisdictions, organizations and service providers have begun voluntarily adopting Privacy by Design (PbD) principles to proactively address risks associated with the collection and processing of minors' personal data. This trend reflects growing awareness of the ethical and reputational imperatives of protecting young users in digital environments, even in the absence of statutory obligations. This section explores real-world instances where PbD has been applied in practice, examining the motivations, mechanisms, and outcomes of such efforts in diverse regulatory contexts.

II. Status of APEC economies

1. Australia

The Children's Online Privacy Code will apply to social media platforms and other online services likely to be accessed by children. The code introduces additional requirements that complement, rather than conflict with, existing regulatory obligations.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

The Office of the Privacy Commissioner of Canada (OPC) actively promotes the integration of Privacy by Design through its official guidance. It emphasizes the importance of identifying and minimizing digital privacy risks to young people as early as possible, stating that "organizations should ensure that privacy and the best interests of young people are built into the product or service right from the design stage" (OPC Joint Resolution, October 2023).

4. Chile

No information was found in relation to this issue.

5. People's Republic of China

No information was found in relation to this issue.

6. Hong Kong, China

The PCPD generally recommends that service providers conduct Privacy Impact Assessments (PIAs) as a best practice to identify, assess, and mitigate potential privacy risks at an early stage. This proactive approach supports the integration of privacy-enhancing measures into the design of products and services before they are implemented or launched.

7. Indonesia

No information was found in relation to this issue.

8. Japan

No information was found in relation to this issue.

9. Republic of Korea

The Personal data Protection Commission (PIPC) recommends the adoption of Privacy by Design (PbD) for services intended for children and adolescents. In practice, several major Korean companies have implemented PbD principles across different digital services. For instance, a second-hand marketplace app that restricts membership for users under the age of 14 includes a feature that allows users to report suspected child users, thereby reinforcing the age restriction policy. In a popular social media application, accounts created by users below a certain age are automatically set to private by default, limiting visibility to friends or followers only. Additionally, users are prompted to choose the desired level of exposure each time they upload content, enhancing control over personal data disclosure. Some services also provide granular options for location tracking permissions—such as “Always Allow,” “Allow While Using the App,” or “Deny”—to support informed privacy choices. Furthermore, if a user initially declares they are under 13 and is subsequently blocked from registering, but later attempts to modify their birthdate from the same IP address, the platform triggers an additional age verification step. These examples illustrate how PbD principles are being voluntarily integrated into service design by Korean companies to enhance privacy protections for younger users, even in the absence of a statutory mandate.

10. Malaysia

No information was found in relation to this issue.

11. Mexico

Currently, there are no specific references or publicly documented examples in Mexico of Privacy by Design (PbD) being applied specifically to the protection of children's or adolescents’ personal data. Although the legal framework promotes PbD principles as a general requirement for all data subjects, concrete implementations tailored to minors have not been clearly identified or widely reported in practice.

12. New Zealand

No requirement for PbD for services that collect, use, store or disclose personal information about children and young people.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

No information was found in relation to this issue.

15. The Republic of the Philippines

No information was found in relation to this issue.

16. The Russian Federation

In practice, companies in Russia have begun to implement child-safe features such as content rating indicators, restricted comment functions, and parent account linkage mechanisms as part of their internal service design. Notably, nine major Russian digital companies—VimpelCom, Gazprom-Media Holding, Kaspersky Lab, MegaFon, MTS, Mail.Ru Group, National Media Group, Rostelecom, and Yandex—have jointly established the Alliance for the Protection of Children in Digital Environments. The alliance aims to foster a child-friendly online environment through creative and secure technologies and digital solutions. Its primary objective is to support children's balanced development by enabling them to fulfill their needs in the digital world, learn how to act responsibly online, and develop strong moral and ethical values.

17. Singapore

No information was found in relation to this issue.

18. Chinese Taipei

No information was found in relation to this issue.

19. Thailand

No information was found in relation to this issue.

20. United States

In the United States, some companies, particularly in the gaming industry and on child-focused platforms, voluntarily implement Privacy by Design (PbD)-aligned measures. These include default "kids mode" settings, minimized data collection, enhanced transparency, accessible support and reporting channels, third-party privacy certifications. Certain companies are under FTC orders that require or prohibit particular conduct.

21. Viet Nam

No information was found in relation to this issue.

III. Comparative Analysis and Implications

Table 6 Practical Implementation of Privacy by Design for Children and Adolescents

	PbD in Practice	Example / Summary

Australia	Yes	Online Privacy Code in development for child-accessed services.
Brunei Darussalam	N/A	No information was found in relation to this issue.
Canada	Yes	OPC promotes PbD for children and adolescents via official guidance.
Chile	N/A	No information was found in relation to this issue.
People's Republic of China	N/A	No information was found in relation to this issue.
Hong Kong, China	Yes (Recommended)	PCPD recommends PIAs as best practice.
Indonesia	N/A	No information was found in relation to this issue.
Japan	N/A	No information was found in relation to this issue.
Republic of Korea	Yes	PbD applied in local apps: default private accounts, location permissions, parental verification.
Malaysia	N/A	No information was found in relation to this issue.
Mexico	No	Legal framework promotes PbD, but no documented child-specific cases.
New Zealand	N/A	No requirement for child-centric PbD
Papua New Guinea	N/A	No information was found in relation to this issue.
Peru	N/A	No information was found in relation to this issue.
The Republic of the Philippines	N/A	No information was found in relation to this issue.
The Russian Federation	Yes	Companies formed alliance and implemented child-safe features.
Singapore	N/A	No information was found in relation to this issue.
Chinese Taipei	N/A	No information was found in relation to this issue.
Thailand	N/A	No information was found in relation to this issue.
United States	Yes	Gaming platforms and YouTube Kids implement PbD-like features voluntarily.

Viet Nam	N/A	No information was found in relation to this issue.

The survey findings indicate that, while documented applications of Privacy by Design (PbD) specifically targeting the protection of children's and adolescents' personal data are limited to a small number of APEC economies, a gradual expansion of voluntary PbD implementation is observable across the region. In jurisdictions where explicit statutory mandates are absent, certain organizations have nonetheless incorporated privacy-enhancing measures into service design through internal governance frameworks, industry self-regulation, and regulatory guidance. Such measures include default high-privacy settings, age assurance mechanisms, parental control features, and data minimization practices. These examples demonstrate that PbD may operate as an effective mechanism for risk mitigation and trust enhancement even in the absence of binding legal obligations.

At the same time, overreliance on voluntary or self-regulatory approaches raises concerns regarding consistency, accountability, and long-term effectiveness. In the absence of clearly articulated regulatory benchmarks or oversight mechanisms, the scope, depth, and effectiveness of PbD implementation may vary considerably across sectors and service providers, potentially resulting in uneven levels of protection for children and adolescents. This variability highlights the need for clearer understanding and open discussion of each jurisdictions' normative expectations, respective best practices, and potential cooperation on coordinating actions to complement voluntary initiatives and promote more even implementation consistent with respective jurisdiction's laws and regulations.

From a regional governance perspective, these findings suggest that APEC economies would benefit from cooperative frameworks that formally recognize and encourage effective PbD practices for children and adolescents. Soft-law instruments, such as non-binding guidelines, best practices, and certification schemes, may play a complementary role in educating on existing regulatory gaps while preserving regulatory flexibility and innovation. Taking these steps, APEC economies may strengthen minimum levels of protection for minors and enhance trust in cross-border digital services.

Chapter 4 Age Assurance Obligations and Methods in Each Economy

As online services become deeply integrated into the daily lives of children and adolescents, concerns about harmful content, data misuse, and online exploitation have intensified. Age assurance has therefore emerged as an essential mechanism to ensure that younger users are granted appropriate protections at the point of access. Regulatory trends across jurisdictions increasingly require service providers to differentiate users by age to implement safeguards and comply with children and adolescents-specific privacy obligations.

Yet age assurance introduces a fundamental tension with the data minimization principle, as assessment mechanisms may involve collecting additional personal information or relying on invasive inference tools. This chapter explores how APEC economies navigate this balance by examining the legal duties imposed on service providers and the specific assurance methods they authorize or encourage.

Section 1 Applicability of Age Assurance to Non-Child-Directed Services

I. Introduction

As children increasingly access a wide range of general online services, regulators are reconsidering whether age verification duties should apply even to platforms not specifically targeting minors. Although these services are designed for a broad audience, they may still expose young users to inappropriate content or features, prompting some economies to explore broader age verification requirements. This section examines whether APEC economies impose such general obligations, the legal thresholds for their application, and how service providers are practically implementing verification measures with data minimization and proportionality principles.

II. Status of APEC economies

1. Australia

No information was found in relation to this issue. The Privacy Act does not impose a general age-verification obligation.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

In Canada, general age verification obligations are not imposed by statute on all services, including those specifically targeting children or adolescents.

4. Chile

The Film Classification Law (Ley 19846, *Ley sobre Calificación de la Producción Cinematográfica*) mandates age-based classification for films and audiovisual content.
In addition, the law stipulates that for films rated for audiences aged 18 and older, the age of viewers must be verified through official identification documents. Theater owners, managers, and admission staff share joint responsibility if they fail to fulfill their duty to verify the age of viewers.

5. People's Republic of China

In general, the Personal Information Protection Law (PIPL) requires that data controllers who are aware that users are under the age of 14 must obtain parental consent before collecting their personal data.

Article 75 of the Law on Protection of Minors stipulates that State shall establish a unified electronic identity authentication system of online games for minors. Online game service providers shall require minors to register and log in online games with their real identity information. Online game service providers shall, in accordance with the relevant regulations and standards of the State, classify game products, provide age-appropriate tips, and take technical measures to prevent minors from having access to inappropriate games or game functions.

Article 31 of the Regulation on the Protection of Minors in Cyberspace requires that online livestreaming service providers shall establish a dynamic verification mechanism of the true identity information of online livestreaming publishers, and shall not provide online live-streaming service to the minors who fail to comply with the legal provisions.

6. Hong Kong, China

There is no overarching regulation that requires service providers to conduct age verification.

7. Indonesia

Even if a platform is not specifically targeted at children or adolescents, GR 17/2025 requires that all electronic service operators (ESOs) establish a minimum age for platform use and clearly communicate it within the service. For example, a pop-up message such as "This service is only available to users aged 13 and above" should be displayed during the sign-up process. This information must be easily understandable to both children and their parents or guardians.

To ensure that age restrictions are properly enforced, ESOs must implement an age verification process during user registration. In doing so, they must collect only the minimum amount of personal data necessary and use it solely for the purpose of verifying age. Once the age verification process is complete, and unless there is a legal obligation to retain the data, it must be promptly and securely deleted.

8. Japan

The APPI provides regulations for the protection of personal data. On the other hand, as noted above, certain individual laws related to the protection of minors stipulate age restrictions and age verification requirements.

9. Republic of Korea

The PIPA does not impose a general age verification obligation. However, since it stipulates protection measures for children under 14 years of age, an age verification process is practically required in cases where the personal data of such children under 14 needs to be processed to fulfill these obligations. Furthermore, there are instances where individual laws in specific sectors mandate the verification of the age and identity of children or adolescents.

10. Malaysia

Under Act 709, there is no general age verification obligation for services not specifically targeting children or adolescents. The definition of "data subject" in the Act applies to all individuals, including minors. While age verification is not mandated, parental consent is required for processing the personal data of minors under 18.

11. Mexico

At the moment, there is no specific legal information available regarding the imposition of general age verification obligations.

12. New Zealand

No requirement for age assurance.

13. Papua New Guinea

There is no legal obligation established through a law with binding legal effect.
However, the currently proposed *Social Media Policy Concept Note* includes provisions under consideration that would require the use of a digital ID (SevisPass) to access certain platforms, thereby introducing restrictions on minors' access to social media services.[14]

14. Peru

[14] https://www.linkedin.com/pulse/papua-new-guinea-social-media-regulation-balancing-child-d4dbf

When seeking consent for the processing of children's and adolescents' personal data, internet platforms or services must make reasonable efforts to verify the identity of the consenting party.[15]

15. The Republic of the Philippines

No information was found in relation to this issue.

16. The Russian Federation

Under Federal Law No. 152-FZ and other content-related legislation, there is no general legal obligation to verify users' age. However, in practice, there is a recognized need to verify age in connection with content that may be accessible to children.
Article 2 of Federal Law No. 436-FZ defines "graphic and/or text symbols of information products" according to the classification system set out in Part 3 of Article 6 of the same law, which governs age-appropriate content labeling.

17. Singapore

The PDPA does not mandate age assurance for organizations. However, organizations may be required to have age assurance under other laws (e.g. Code of Practice for Online Safety – App Distribution Services). In this regard, organizations are expected to implement age assurance in accordance with the PDPA and any relevant guidelines including the Advisory Guidelines on The PDPA for Children's Personal Data in The Digital Environment which stipulate, among other requirements, that organizations should practice data minimization for age assurance purposes.

18. Chinese Taipei

There is no obligation established through a legally binding law.

19. Thailand

No information was found in relation to this issue.

20. United States

No broad, general age verification obligation exists. COPPA applies only to services directed to children under 13 or with actual knowledge they collect personal data from such children. The United States Federal Trade Commission recently issued a COPPA policy statement to incentivize the use of age verification technologies to protect children online.[16] The policy

[15] https://insightplus.bakermckenzie.com/bm/data-technology/peru-new-regulations-of-the-personal-data-protection-law_1

[16] See FTC Press Release available at: https://www.ftc.gov/news-events/news/press-releases/2026/02/ftc-issues-coppa-policy-statement-incentivize-use-age-verification-

statement announces an enforcement approach regarding the collection, use, and disclosure of personal data to determine the age of a user. The policy statement states that the Commission will not bring an enforcement action under the COPPA Rule against operators of general audience sites and services and mixed audience sites and services that collect, use, or disclose personal information for the sole purpose of determining a user's age without first obtaining verifiable parental consent—if they comply with certain conditions, specifically that they:

- do not use or disclose information collected for age verification purposes for any purpose except to determine a user's age;
- do not retain this information longer than necessary to fulfill the age verification purposes, and delete such information promptly thereafter;
- disclose information collected for age verification purposes only to those third parties the operator has taken reasonable steps to determine are capable of maintaining the confidentiality, security, and integrity of the information, including by obtaining certain written assurances from those third parties;
- provide clear notice to parents and children of the information collected for age verification purposes;
- employ reasonable security safeguards for information collected for age verification purposes; and
- take reasonable steps to determine that any product, service, method, or third party utilized for age verification purposes is likely to provide reasonably accurate results as to the user's age.

21. Viet Nam

There is no general obligation to verify age that applies to all services, including those not specifically designed for children.

III. Comparative Analysis and Implications

Table 7 Applicability of Age Verification to Non-Child-Directed Services

APEC Economy	Age Verification Obligation
Australia	No – No general obligation; no statutory age-verification requirement.
Brunei Darussalam	No information was found in relation to this issue.
Canada	No statutory obligation
Chile	Yes – required for films rated 18+
People's Republic of China	No general obligation under PIPL; but sectoral mandates
Hong Kong, China	No general obligation

technologies-protect-children

Indonesia	Yes – GR 17/2025 requires for all ESOs
Japan	Yes – in sectoral laws
Republic of Korea	No general obligation; but under-14 verification required in practice, plus sectoral mandates
Malaysia	No general requirement; parental consent <18
Mexico	No specific law
New Zealand	No legal requirement
Papua New Guinea	Proposed in draft social media policy
Peru	Yes – platforms must verify consent-giver identity
The Republic of the Philippines	N/A - No information was found in relation to this issue
The Russian Federation	No legal requirement, but needed for content labeling
Singapore	No legal obligation, but recommended for protection
Chinese Taipei	No binding obligation
Thailand	N/A - No information was found in relation to this issue
United States	Only if directed to 13 or younger or actual knowledge collected from 13 or younger (COPPA)
Viet Nam	No general requirement

The comparative analysis shows that most APEC economies do not impose general age verification obligations on all online services. Such duties typically arise only where services are directed at children or adolescents, where operators have knowledge of their use, or where content is subject to statutory age-based restrictions. Only a limited number of economies have adopted broader, cross-sectoral age verification requirements.

This restrained regulatory approach reflects concerns regarding proportionality, technical feasibility, and compliance with the data minimization principle. Mandatory age verification may require the collection of additional personal data or the use of intrusive identification methods, prompting many economies to favor sector-specific rules or contextual obligations linked to parental consent or content classification rather than universal mandates.

Nevertheless, the survey indicates an implicit expectation that service providers assess users' age where legal protections depend on age thresholds. Even in the absence of explicit statutory requirements, liability regimes and child protection frameworks effectively encourage the adoption of age assurance measures in practice. These findings underscore the importance of privacy-preserving, risk-based approaches to age verification that balance child protection objectives with data protection and innovation.

Section 2 Specific Categories Subject to Strict Verification

I. Introduction

Even where no general age verification obligation applies to all online services, many economies still enforce such requirements for specific high-risk categories. Platforms offering adult content, gambling, or other legally restricted activities are often subject to stricter age assurance duties due to the elevated risks they pose to children and adolescents. These sector-specific rules reflect a regulatory view that certain environments demand stronger controls at the point of access, even in the absence of broader, industry-wide mandates.

This section examines how APEC economies identify these high-risk categories, the legal standards that trigger mandatory age verification, and the types of verification methods required from service providers.

II. Status of APEC economies

1. Australia

The Online Safety Amendment (Social Media Minimum Age) Bill 2024 will introduce mandatory age assurance requirements for social media services to prevent access by children under 16. These obligations will take effect from December 2025.

2. Brunei Darussalam

No explicit obligations, however, adult content itself is strictly regulated under Islamic law.

3. Canada

Age verification or declaration requirements typically apply only to industries where age restricted goods, services, or content are provided by law (e.g., alcohol, tobacco, cannabis, gambling, or explicit/adult content), or where a law or regulation specifically requires it.

4. Chile

Article 367 of the Criminal Code defines it as a criminal offense to use a technical device to transmit visual or audio content of a sexual nature to minors under the age of 18, and such conduct is punishable by imprisonment. As a result, online platforms and internet services may have practical incentives to implement age verification mechanisms. However, platforms that unintentionally facilitate the commission of such crimes are not subject to criminal liability.[17]

5. People's Republic of China

Article 75 the Law on Protection of Minors stipulates that the State shall establish a unified electronic identity authentication system of online games for minors. Online game service providers shall require minors to register and log in online games with their real identity information. Online game service providers shall, in accordance with the relevant regulations

[17] https://www.globalchildexploitationpolicy.org/content/dam/gpp/legal-research/Chile%20-%20Legal%20Research.pdf

and standards of the State, classify game products, provide age-appropriate tips, and take technical measures to prevent minors from having access to inappropriate games or game functions.
Article 76 of the same law stipulates that live streaming service providers are prohibited from offering account registration services for live streaming to minors under the age of 16.

6. Hong Kong, China

Sector-specific regulations do exist for services that are explicitly targeted at adults. For example, the Dutiable Commodities Ordinance (Cap. 109) and the Dutiable Commodities (Liquor) Regulations (Cap. 109B) specifically prohibit the sale and supply of intoxicating liquor to minors in the course of business, whether through face-to-face transactions or remote means like e-commerce. Sellers are recommended to inspect the buyer's proof of identity for age verification when in doubt.

7. Indonesia

According to the amended Electronic Information and Transaction Law (EIT Law, UU No. 11/2008) of 2024, electronic system operators are required to clearly specify the minimum age at which children can use their products or services and to establish mechanisms to verify whether the user is a child. [18]

For the reference, regulations are currently being developed to establish a minimum age for the use of social networking services (SNS). [19]

8. Japan

In general, for categories where age restrictions are typically imposed, such as the following, it is considered that individual laws or ordinances mandate age verification:

- Adult content
- Dating and matching applications
- Sale of alcohol and tobacco
- Online lotteries and gambling-related services, etc.

9. Republic of Korea

There are cases where individual laws stipulate age verification obligations depending on the service type. For example:

[18] https://www.arma-law.com/news-event/newsflash/newsflash/second-eit-law-amendment-law-no-1-of-2024

[19] https://www.reuters.com/world/asia-pacific/indonesia-planning-minimum-age-limit-social-media-users-minister-says-2025-01-14/

- Article 16 of the Juvenile Protection Act requires confirmation of age and identity when selling or lending media harmful to minors.
- Article 12-3 of the Game Industry Promotion Act imposes an obligation to verify real name, age, and identity during user registration for game services.
- Article 44-7, Paragraph 1, Subparagraph 5 of the Network Act prohibits the for-profit sale of information deemed harmful to minors without fulfilling legal obligations such as age verification.

10. Malaysia

No information was found in relation to this issue.

11. Mexico

Although such obligation is not established under data protection law, there are other legal provisions in place to safeguard children and adolescents.

12. New Zealand

No, no such obligation exists under New Zealand Privacy law. Obligations outside of the privacy laws will apply where age restricted products are being sold or made available.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

Under no circumstances may consent be granted for the processing of a minor's personal data for the purpose of accessing goods or services intended for adults.[20]

15. The Republic of the Philippines

The Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act requires all online providers of adult content to implement an anonymous age verification process before granting access to such content, ensuring minors cannot access sexually explicit materials online. (Section 35)

The Department of Trade and Industry also issued Department Administrative Order No. 25-04, s. 2025 which requires online platforms selling vaporized nicotine and non-nicotine products to verify age of buyers to prevent sales to those under 18 years old. (Section 2)

[20] https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/latin-america/peru/topics/legal-bases-for-processing-of-personal-data

16. The Russian Federation

In certain areas such as adult content and the distribution of harmful information, age verification is effectively required.

No. 436-FZ, Article 2:

- “6) information products for children - the information products corresponding on subject, content and decorating to physical, mental, spiritual and moral development of children;
- 7) information doing harm to health and (or) development of children, - information (including containing in information products for children) which distribution among children is forbidden or limited according to this Federal Law;

8) information of pornographic nature - information presented in the form naturalistic images or descriptions of genitals of the person and (or) sexual connection or action of sexual nature, comparable to sexual connection, including such action made concerning animal”

17. Singapore

To ensure the online safety of children and adolescents, the Infocomm Media Development Authority (IMDA) enacted the *Code of Practice for Online Safety for App Distribution Services* (effective from 31 March 2025). This regulation requires designated app stores with significant reach or impact—such as the Apple App Store, Google Play Store, Huawei AppGallery, Microsoft Store, and Samsung Galaxy Store—to have in place systems and processes, including age verification, or other means of age assurance to establish the age or age range of users with reasonable accuracy.[21]

18. Chinese Taipei

No information was found in relation to this issue.

19. Thailand

No information was found in relation to this issue.

20. United States

State laws often require age verification or age gating for alcohol, tobacco, gambling, and adult/obscene material. States such as Virginia, California, and Texas have enacted laws mandating age verification for providers of pornographic and certain other content and services.

[21] https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/online-safety-code-of-practice-for-app-distribution-services

21. Viet Nam

There is no specific list of services for which age verification is explicitly required.

Age verification is typically required or strongly encouraged for services whose content or nature may be harmful or inappropriate for children, including:

- **Online games**: Especially those containing elements of violence, gambling, or other content unsuitable for children.
- **Digital content (films, music, e-books)**: Platforms providing adult content (sensitive material) are required to implement age verification mechanisms to prevent children's access.
- **Financial or transactional services**: These services generally require users to be of legal age in accordance with the law in order to carry out valid transactions.

III. Comparative Analysis and Implications

Table 8 Specific Categories Subject to Strict Verification

APEC Economy	Age Verification for Adult/Restricted Services
Australia	N/A - Regulation targets child access in specific field will be introduced
Brunei Darussalam	No explicit obligation; Not allowed under Islamic law
Canada	Yes – only for age-restricted industries
Chile	Yes – Criminal Code Article 367
People's Republic of China	Yes – mandatory for games & livestream under MPL
Hong Kong, China	Yes – liquor laws require age proof
Indonesia	Yes – EIT Law 2024 requires age mechanisms
Japan	Yes – by individual laws (adult, gambling, etc.)
Republic of Korea	Yes – by law for harmful media, games, content
Malaysia	N/A - No information was found in relation to this issue
Mexico	Yes – No explicit age-verification obligation; but other legal provisions exist
New Zealand	No under privacy law; yes for adult goods
Papua New Guinea	N/A - No information was found in relation to this issue
Peru	No explicit age-verification mandate; minors cannot consent to access adult services
The Republic of the Philippines	Yes – required under OSAEC, nicotine sales rules
The Russian Federation	Yes – for harmful/adult information

Singapore	Yes – for app stores (IMDA online safety code)
Chinese Taipei	N/A - No information was found in relation to this issue
Thailand	Yes
United States	Yes – for alcohol, porn, gambling, etc.
Viet Nam	Yes – strongly encouraged for adult/harmful content

The comparative analysis indicates that, although general age verification obligations remain limited across APEC economies, sector-specific age verification requirements are widely adopted and more consistently enforced. Most economies impose mandatory or de facto age verification duties in high-risk sectors, such as adult content, gambling, gaming, alcohol, and other age-restricted goods or services. These obligations are typically grounded in criminal law, content regulation, consumer protection, or sectoral licensing frameworks rather than in general data protection statutes.

This targeted regulatory approach reflects a deliberate policy choice to concentrate age verification requirements in environments where the risk of harm to children and adolescents is most pronounced. By limiting mandatory verification to clearly defined high-risk contexts, regulators seek to protect them while avoiding the privacy, proportionality, and feasibility concerns associated with economy-wide age verification mandates. Sector-specific regimes also allow for differentiated verification standards that are tailored to the nature and severity of the underlying risks.

At the same time, the survey demonstrates that even in jurisdictions without explicit cross-sector age verification mandates, legal responsibilities for content moderation, criminal liability, or consent validity effectively incentivize platforms to implement age assurance mechanisms in practice. This convergence suggests an emerging functional standard in which age verification is increasingly expected for services that expose children to heightened risks, regardless of whether such obligations are expressly codified. From a regional perspective, these findings highlight opportunities to encourage sharing perspectives on developing guidance on proportionate and privacy-preserving age verification practices, consistent with domestic law, that can be adapted across high-risk sectors.

Section 3 Adopted Mechanisms for Age Verification

I. Introduction

As age verification obligations become more common across digital services, APEC economies specify which methods service providers must or may adopt. These methods vary widely in intrusiveness and reliability, from simple document checks using ID cards or passports to more sophisticated approaches such as third-party verification, biometric estimation, or AI-based facial and voice recognition. Each method presents different implications for accuracy, user experience, and the protection of children's and adolescents' personal data. This section surveys the range of age verification techniques recognized within APEC economies and assesses the regulatory preferences that guide their adoption.

II. Status of APEC economies

1. Australia

The laws do not prescribe specific age-verification methods.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

In regulated sectors, organizations typically use a combination of government issued photo ID (online upload or in person), third-party verification services, or database checks to satisfy age verification requirements contingent on relevant provincial laws.

4. Chile

Age must be verified through official documents (such as an identity card).[22]

5. People's Republic of China

The tone of Article 31 of the PIPL emphasizes not the process of taking steps to obtain "consent of the parents or other guardians of the minors," but rather the outcome—whether "consent of the parents or other guardians of the minors" has actually been secured. In other words, personal information processors must formally obtain consent of the parents or other guardians of the minors; making reasonable efforts alone is insufficient. If the processor cannot prove that verified consent has been obtained, they will be held responsible for processing a child's personal information.

6. Hong Kong, China

See the response in 3.2 above. Sector-specific regulations do exist for services that are explicitly targeted at adults. For example, the Dutiable Commodities Ordinance (Cap. 109) and the Dutiable Commodities (Liquor) Regulations (Cap. 109B) specifically prohibit the sale and supply of intoxicating liquor to minors in the course of business, whether through face-to-face transactions or remote means like e-commerce. Sellers are recommended to inspect the buyer's proof of identity for age verification when in doubt.

7. Indonesia

No information was found in relation to this issue.

[22] https://www.globalchildexploitationpolicy.org/content/dam/gpp/legal-research/Chile%20-%20Legal%20Research.pdf

8. Japan

The following age verification methods are generally considered to be adopted:

- Submission of official identification documents
- Self-declaration, etc.

9. Republic of Korea

While specific methods are stipulated differently depending on individual laws and regulations, Article 17 of the Enforcement Decree of the Juvenile Protection Act, which is the most representative regulation, requires age verification by the following methods when selling or lending media harmful to minors:

- Identity verification through face-to-face interaction or confirmation of an ID copy received via fax or mail.
- Verifiable electronic signature (certificate in accordance with the Electronic Signature Act).
- Alternative means of identity verification (methods to confirm identity without using a resident registration number).
- Credit card verification.
- Mobile phone verification (age and identity must be confirmed by adding methods such as text message transmission or automated voice response via mobile phone).
- Other equivalent methods.

10. Malaysia

No information was found in relation to this issue.

11. Mexico

Although such obligation is not established under data protection law, there are other legal provisions in place to safeguard children and adolescents.

12. New Zealand

The Biometrics Code (published in 2025) provides rules around use of biometrics which would include the use of biometrics for the purposes of age verification.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

Under Law No. 29733, no specific method of age verification is required.

15. The Republic of the Philippines

For Department Administrative Order No. 25- 04, s. 2025, age gating measures may include:

- Confirmation or re-encoding of some of the data stated in the consumer's or viewer's government-issued identification document or card submitted at the Registration process provided herein;
- Encoding of a One-Time Password (OTP) or Personal Identification Number (PIN) sent by the internet website or e-commerce and/or similar media platform to the consumer or viewer:
- Use of facial recognition technology or biometrics;
- Use of artificial intelligence (AI), programs or algorithms to detect underage attempts to access, or purchase the covered products;
- Use of artificial intelligence (AI), or image recognition programs or technologies to prevent deceptive posts of non-compliant images; or
- Use of geofencing technology to restrict access to the covered products in locations frequented by individuals below eighteen (18) years of age.

16. The Russian Federation

No information was found in relation to this issue.

17. Singapore

Age Assurance refers to systems or processes to establish a person's age or age range, including[23]:

:

- **Age Estimation**: Relies on analysis of biological or behavioural features of humans that vary with age to establish the likely age or age range e.g. facial age analysis or voice modelling. It may use Artificial Intelligence or machine learning technology.
- **Age Verification**: Relies on authoritative sources of checking a user's date of birth or year of birth to determine the age or age range of a user e.g. Digital ID, passport, driving license.
- **Age Inference**: Relies on analysis of verifiable contextual, behavioural or transactional signals to draw reasonable conclusions about age e.g. school enrolment record, financial transaction/possession of a valid credit card, possession of a seniors' concession card, account tenure, content engagement, or account activity patterns.
-

18. Chinese Taipei

[23] https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/internet/online-safety

No information was found in relation to this issue.

19. Thailand

No information was found in relation to this issue

20. United States

No information was found in relation to this issue. Under COPPA, operators must “make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology.” Acceptable methods include payment notification to parents, print-and-send forms signed by parents, government-issued ID, and other measures.

21. Viet Nam

Decree No. 13/2023/ND-CP does not specify mandatory methods for age verification.

Common and accepted methods for age verification include:

- **Using personal identification information**: Services may request users to enter their local ID/citizen identification number for cross-checking against the economy’s population database (if they have lawful access and are duly authorized) or require a photo/scan of the ID card.
- **Verification through parents/legal guardians**: When registering for children, services may require consent and age confirmation from the child’s parent or legal guardian.

III. Comparative Analysis and Implications

Table 9 Adopted Mechanisms for Age Verification

APEC Economy	Age Verification Methods
Australia	No specific method prescribed under law
Brunei Darussalam	No information was found in relation to this issue
Canada	Gov ID, 3rd party verification services, database checks
Chile	Official documents (ID card)
People’s Republic of China	Verified parental consent required; no specific age-verification method defined.
Hong Kong, China	Proof of ID recommended under Sector-specific (liquor law)
Indonesia	No information was found in relation to this issue
Japan	ID submission, self-declaration

Republic of Korea	Face-to-face, ID copy, electronic signature, credit card, phone verification
Malaysia	No information was found in relation to this issue
Mexico	No specific method identified; other child-protection laws exist
New Zealand	Use biometrics for the purpose of age verification (Biometrics Code published in 2025)
Papua New Guinea	No information was found in relation to this issue
Peru	No legally specified method
The Republic of the Philippines	Gov ID, OTP, facial recognition, AI detection, geofencing
The Russian Federation	No information was found in relation to this issue
Singapore	AI-based estimation, Gov/digital ID, credit card
Chinese Taipei	No information was found in relation to this issue
Thailand	No information was found in relation to this issue
United States	COPPA: payment notification, ID, signed forms
Viet Nam	ID cross-check, guardian consent, ID photo upload

The comparative analysis reveals substantial divergence across APEC economies with respect to the age verification methods that are legally prescribed, permitted, or recommended. In many jurisdictions, no specific verification techniques are mandated, leaving service providers with broad discretion in determining appropriate mechanisms. Where legal provisions do exist, government-issued identification documents remain the most commonly recognized method, reflecting their perceived reliability and legal certainty in establishing age.

At the same time, the survey highlights a gradual expansion of alternative and technology-based approaches, including third-party verification services, credit card authentication, one-time passwords, biometric tools, and AI-based age estimation. These methods are often introduced in sector-specific regulations or administrative guidance rather than in primary legislation. While such approaches may reduce friction or improve scalability, they also raise heightened concerns regarding accuracy, bias, data minimization, and the long-term retention of sensitive biometric data.

From a regulatory perspective, the absence of harmonized standards regarding acceptable age verification methods creates legal uncertainty for service providers operating across borders and may result in inconsistent levels of protection for children and adolescents. A risk-based approach that allows for differentiated methods depending on service context and harm potential may offer a more sustainable regulatory path while safeguarding children's rights and personal data.

Section 4 Non-Statutory Guidelines and Industry Practices for Age Verification

I. Introduction

Even without legally mandated age verification requirements, regulators often issue non-binding guidelines encouraging service providers to adopt protective measures for children and adolescents. These recommendations may include using light-touch age estimation tools, implementing parental controls, or integrating third-party verification services in high-risk contexts. As online platforms face growing societal pressure to ensure child safety, many companies voluntarily adopt such measures to demonstrate accountability and mitigate potential risks. This section examines the regulatory guidance and industry-led practices emerging across APEC economies, focusing on how companies operationalize voluntary age verification in the absence of formal obligations.

II. Status of APEC economies

1. Australia

No information was found in relation to this issue.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

The OPC's guidance on children's privacy online recommends that organizations take reasonable steps to determine the age of users when their services are directed at or likely used by children.

The OPC has completed a public consultation on age assurance in 2024 to inform the OPC's 2024-2027 priorities citing age assurance as a key issue for the OPC.

4. Chile

No information was found in relation to this issue.

5. People's Republic of China

No information was found in relation to this issue.

6. Hong Kong, China

Sector-specific regulations do exist for services that are explicitly targeted at adults. For example, the Dutiable Commodities Ordinance (Cap. 109) and the Dutiable Commodities (Liquor) Regulations (Cap. 109B) specifically prohibit the sale and supply of intoxicating liquor to minors in the course of business, whether through face-to-face transactions or remote means like e-commerce. Sellers are recommended to inspect the buyer's proof of identity for age verification when in doubt.

7. Indonesia

No information was found in relation to this issue.

8. Japan

No information was found in relation to this issue.

9. Republic of Korea

The PIPC, through its "Guide to Personal Data Protection for Children and Adolescents," recommends that if a data controller can reasonably anticipate that a service will be used by children and adolescents, based on a comprehensive review of its content and delivery methods, they should verify the user's age to determine if they are a child under 14 years old before providing the service.

Specifically, when offering services to children or adolescents that require a membership registration process, data controllers are advised to guide users to access the service only after completing an age verification step. This can be done by having the user directly enter their legal birthdate or self-check a box labeled "14 years old or older."

Additionally, the PIPC recommends implementing reasonable measures to prevent children under 14 from falsely stating their age for unauthorized use. Examples include requiring additional age verification steps if fraudulent registration is suspected, or providing a feature for users to report suspected underage users through peer monitoring.

10. Malaysia

Although Act 709 does not require age verification, companies often implement measures like parental consent, date of birth verification during registration and payment verification to protect minors' personal data. These practices are especially common in social media, e-commerce and gaming platforms to ensure compliance with privacy protections for children and adolescents.

11. Mexico

Yes, non-binding recommendations have been issued by regulatory authorities to guide companies implementing age verification measures.

12. New Zealand

The Biometrics Code (published in 2025) provides rules around use of biometrics which would include the use of biometrics for the purposes of age verification.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

In the case of Google, only users aged 14 or older can create and manage an account. If it is determined that a user does not meet the age requirement, they must either set up parental supervision within 14 days or verify their age using an official form of identification (e.g., local ID, passport) or a credit card. If they fail to do so, the account will be suspended and eventually deleted.[24][25]

15. The Republic of the Philippines

The NPC Advisory on Guidelines on Child Oriented Transparency recommends the implementation of age assurance mechanisms to determine the age range of users as a tool to adopt age-appropriate practices when processing children's personal data. (Section 2)

16. The Russian Federation

No information was found in relation to this issue.

17. Singapore

No information was found in relation to this issue.

18. Chinese Taipei

No information was found in relation to this issue.

19. Thailand

No information was found in relation to this issue.

20. United States

FTC staff has referenced reasonable measures to prevent children circumventing age gates in its official publications.

21. Viet Nam

[24] https://support.google.com/accounts/answer/1350409#zippy=

[25] https://support.google.com/accounts/answer/1333913

Although there is no legal obligation, there are recommendations from regulatory authorities as well as practical measures adopted by companies concerning age verification. Specifically:

Recommendations from regulatory authorities:

- The Ministry of Public Security and the Ministry of Science and Technology have recommended that online service providers implement child protection measures, including age verification of users, to prevent children from accessing harmful content or engaging in inappropriate activities.

Practical measures implemented by companies:

- Requiring users to enter their year of birth during registration.
- Displaying warnings or restricting access to content classified as inappropriate for children.
- Providing tools for parents to manage their children's accounts, including access restrictions, screen time controls, and privacy settings.

III. Comparative Analysis and Implications

The following table indicates whether there are regulatory recommendations or practical measures adopted by companies regarding age verification each APEC economy.

Table 10 Non-Statutory Guidelines and Industry Practices for Age Verification

APEC Economy	Age Verification Policy/Guidance
Australia	No information was found in relation to this issue
Brunei Darussalam	No information was found in relation to this issue
Canada	OPC recommends age assurance; public consultation held
Chile	No information was found in relation to this issue
People's Republic of China	No information was found in relation to this issue
Hong Kong, China	Sector-specific ID check recommended (liquor sales)
Indonesia	No information was found in relation to this issue
Japan	No information was found in relation to this issue
Republic of Korea	PIPC guide recommends proactive age checks, safeguards
Malaysia	DOB checks, parental consent common practice
Mexico	Yes – non-binding recommendations issued by authorities
New Zealand	Biometrics Code includes the use of biometrics for the purpose of age verification
Papua New Guinea	No information was found in relation to this issue

Peru	Platform practice: Google requires age verification or parental supervision
The Republic of the Philippines	NPC Advisory recommends age assurance tools
The Russian Federation	No information was found in relation to this issue
Singapore	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment
Chinese Taipei	No information was found in relation to this issue
Thailand	No information was found in relation to this issue
United States	FTC recommends age gates + monitoring + parental alerts
Viet Nam	Regulators and companies recommend age checks + controls

The comparative analysis indicates that, across most APEC economies, voluntary or recommended age verification practices remain limited and unevenly developed. In many jurisdictions, regulatory authorities have not issued formal guidance on age assurance in the absence of statutory obligations, resulting in a lack of consistent expectations for service providers. Where recommendations do exist, they are typically articulated through non-binding guidelines, advisories, or consultation documents rather than enforceable legal instruments.

Nevertheless, the survey identifies a small but notable group of economies in which regulators actively encourage proactive age assurance measures, particularly where services are directed at or likely to be accessed by children and adolescents. Such guidance often emphasizes reasonable, proportionate steps, such as self-declared age inputs, parental notification, or graduated verification mechanisms, aimed at reducing circumvention risks without imposing excessive data collection burdens. These approaches reflect an effort to balance child protection objectives with privacy, feasibility, and innovation considerations.

In parallel, certain companies have independently adopted age verification or age assurance practices as part of their internal risk management and safety strategies, even in the absence of legal mandates. Platform-driven measures, including age gates, parental supervision tools, and account suspension mechanisms, demonstrate how private governance can supplement regulatory gaps. However, reliance on voluntary or company-specific practices also raises concerns regarding transparency, accountability, and unequal levels of protection. From a regional perspective, these findings underscore the growing role of soft-law instruments and industry initiatives, while opportunities to encourage sharing perspectives regarding guidance to ensure that voluntary age assurance practices contribute meaningfully to the protection of children and adolescents across the digital ecosystem.

Chapter 5 Separate Legal Bases Required for Processing Children or Adolescents' Personal Data

Compared to adults, children and adolescents have limitations in fully understanding the meaning and consequences of the processing of their personal data and in exercising their right to self-determination. Therefore, it is difficult to sufficiently protect their rights with general personal data processing standards alone. Accordingly, discussions are emerging that special protection is necessary for the processing of personal data of children and adolescents, such as requiring a separate legal basis. In this context, this section intends to examine the details of the special protections granted across APEC economies.

Section 1 Differentiating the Legal Grounds for Minors and Adults

I. Introduction

The processing of personal data belonging to children and adolescents necessitates a legal framework that is distinct from and more stringent than that applied to adults. For example, the consent mechanism is predicated on the assumption that the data subject is capable of making a free and informed decision. This assumption is frequently untenable in the case of minors, whose underdeveloped cognitive abilities, limited understanding of long-term consequences, and heightened vulnerability to commercial or social pressures render them unable to provide meaningful consent. Consequently, a differentiated approach to establishing a lawful basis for processing may serve a fundamental requirement for upholding their rights.

II. Status of APEC economies

1. Australia

While the Privacy Act does not establish differing obligations for regulated entities based on an individual's age, there is a distinction in relation to consent. The Children's Online Privacy Code (currently being developed), may provide further specification on how existing requirements are to be complied with, with respect to children.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

No separate lawful bases for adults vs. minors, consent is always required under PIPEDA with limited exceptions most notably for legal, security, investigative, emergency, or business

transaction situations. However, as will be discussed in Chapter 5, Section 2, a consent from a legal representative is recognized as a legal basis for processing personal data of minors.

4. Chile

The Data Protection Law introduces a "best interest" standard for the protection of children and adolescents' personal data.

5. People's Republic of China

Article 31 of the PIPL requires that to process the personal information of minors under the age of 14, personal information processors shall obtain the consent of the parents or other guardians of the minors.

6. Hong Kong, China

The PDPO is applicable to all age groups, including children and adolescents. There is no differentiation on the bases for processing adults' and children's personal data. In the event that the data subject is a minor (i.e. persons who have not attained the age of 18), a "relevant person" (being a person who has parental responsibility for the minor as stipulated in s.2 of the PDPO) could give the prescribed consent on behalf of the minor if the minor's personal data is to be used for a purpose other than and not directly related to the original purpose(s) for which such data is being collected.

7. Indonesia

The PDP law requires parental consent before collecting personal data of children and adolescents, and GR 17/2025 further emphasizes that this consent must be clear, explicit, and responsible. According to Article 7, par (1) of GR 17/2025, electronic service operators must obtain the consent of a parent or legal guardian to process the personal data of children and adolescents.

8. Japan

Under the APPI, no explicit legal distinction is made between adults and minors with respect to the processing of personal data. However, APPI Guidelines set forth specific provisions regarding the requirement of consent in cases where the data subject is a minor.

9. Republic of Korea

The PIPA does not, in principle, separately stipulate legal bases for processing personal data for children or adolescents versus adults. However, a difference exists in that children under 14 years of age require the consent of their legal guardian.

10. Malaysia

For children and adolescents under 18, the primary lawful basis for processing their personal data is parental consent, due to their vulnerability and limited understanding of data processing implications.

11. Mexico

There is no distinction in relation to the legal bases for the processing of children's and adolescents' personal data and those applicable for adults, since consent is the main legal basis by rule for the processing of personal data regardless of the age of the data subject, and the exceptions for the use of consent are all applicable to both adults or underage data subjects. However, a particular difference, in the processing of personal data is the collection of consent for the processing of children's and adolescents' personal data, which requires consent from the legal guardian of the data subject, that shall comply with the superior interest of child, and the provisions of the Mexican civil law, and the LGDNNA.

12. New Zealand

There is no distinction in relation to the legal bases available for the processing of children's and adolescents' personal data and those applicable for adults. However, as will be discussed in the Chapter 5, Section 2, an authorization (consent) from a legal representative is exceptionally recognized as a legal basis for collecting, using, and disclosing personal data of minors.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

No information was found in relation to this issue.

15. The Republic of the Philippines

No distinctions under the Data Privacy Act. However, as will be discussed in Chapter 5, Section 2, a consent from a legal representative is recognized as a legal basis for processing personal data of minors.

16. The Russian Federation

Federal Law No.152-FZ does not explicitly distinguish the legal basis for processing between adults and minors, but it requires the consent of a parent or legal guardian for processing minors' personal data.

17. Singapore

The PDPC considers that a child between 13 and 17 may give valid consent, when the policies on the collection, use and disclosure of the child's personal data, as well as the withdrawal of consent, are readily understandable by them. This includes ensuring that the child understand the consequences of providing and withdrawing consent. However, where an organization has reason to believe that a child does not have sufficient understanding of the nature and consequences of giving consent, the organization should obtain consent from the child's parent or guardian. Organizations should also ensure that children are able to withdraw consent for their personal data as easily as providing consent for their personal data.

18. Chinese Taipei

The legal basis for processing may or may not be the party's consent, depending on the age. For children and adolescents between 7 and 18, consent is not valid without the consent of a person with parental responsibility, and for children under 7, only a person with parental responsibility can provide consent.

19. Thailand

The PDPA distinguishes the legal basis for processing between adults and children. For minors under 20, separate requirements for consent apply depending on the situation. For minors under 10, consent requirements are unconditional.

20. United States

Under COPPA, strict verifiable parental consent is required to collect personal data from minors under 13. In contrast, for adults, consent is not usually a prerequisite for personal data collection except, for example, for special categories such as opt-in marketing under certain state laws or where necessary to prevent unfair or deceptive conduct.

21. Viet Nam

Currently, Government Decree No. 13/2020 includes provisions on the processing of children's personal data (Article 20). However, there is no specific classification between young children and adolescents.

III. Comparative Analysis and Implications

The following table indicates whether APEC economies have established distinct legal bases for processing the personal data of minors compared to adults.

Table 11 Differentiating the Legal Grounds for Minors and Adults

APEC Economy	Differentiated Legal Basis for Minors vs Adults (O/X)
Australia	O
Brunei Darussalam	N/A (No information was found in relation to this issue)

Canada	O
Chile	O
People's Republic of China	O
Hong Kong, China	O
Indonesia	O
Japan	O
Republic of Korea	O
Malaysia	O
Mexico	O
New Zealand	O (by exception)
Papua New Guinea	N/A (No information was found in relation to this issue)
Peru	N/A (No information was found in relation to this issue)
The Republic of the Philippines	O
The Russian Federation	O
Singapore	O
Chinese Taipei	O
Thailand	O
United States	O
Viet Nam	O

The comparative analysis demonstrates that a clear majority of APEC economies recognize the need to differentiate the legal bases for processing the personal data of children and adolescents from those applicable to adults. While many data protection frameworks formally maintain consent as the primary lawful basis regardless of age, they impose heightened requirements in the case of minors, most commonly through mandatory parental or legal guardian consent. This approach reflects a shared regulatory assessment that minors generally lack the capacity to provide free and informed consent equivalent to that of adults.

Although the degree of differentiation varies across jurisdictions, a common structural pattern emerges. Rather than establishing entirely separate legal bases, most economies modify the operation of consent by introducing age thresholds, substitutive consent mechanisms, or enhanced safeguards grounded in the best interests of the children and adolescents. In some jurisdictions, this differentiation is further refined by distinguishing between children and adolescents, while others adopt a uniform rule for all minors. These variations illustrate differing domestic assessments of children's evolving capacities, yet converge on the principle that adult-centric consent models are insufficient for protecting children and adolescents' data rights.

From a regulatory and compliance perspective, these findings signal a decisive shift toward specialized protective regimes for children and adolescents. For global service providers, the implication is that a single, uniform legal basis for personal data processing can no longer be assumed across user populations. Organizations must design compliance frameworks capable of identifying children and adolescents, applying differentiated legal bases, and operationalizing parental or guardian involvement where required. Failure to account for these distinctions not only increases legal risk but also undermines emerging international norms that prioritize the heightened protection of children and adolescents' personal data.

Section 2 Recognized Legal Bases for Processing Children's and Adolescents' Personal Data

I. Introduction

If a legal system does differentiate, it is crucial to understand the *substance* of that differentiation. This section aims to identify the specific legal tools and mechanisms—such as the consent of a legal representative—that are authorized for processing a minor's data.

II. Status of APEC economies

1. Australia

For consent to be valid, an individual must have the capacity to consent. The capacity to consent generally means that an individual is capable of understanding the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgment and how to communicate a consent decision. If an individual under the age of 18 lacks the capacity or maturity to understand what is being proposed, it may be considered appropriate for a parent or guardian to consent on their behalf.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

No information was found in relation to this issue.

4. Chile

Consent from a parent or legal guardian, or in situations explicitly authorized by law.

5. People's Republic of China

Article 31 of the PIPL requires separate or written consent from a parent for processing a child's personal data.

6. Hong Kong, China

In the event that the data subject is a minor, a "relevant person" (being a person who has parental responsibility for the minor as stipulated in s.2 of the PDPO) could give the prescribed

consent on behalf of the minor if the minor's personal data is to be used for a purpose other than and not directly related to the original purpose(s) for which such data is being collected.

7. Indonesia

The PDP law requires parental consent before collecting personal data of children and adolescents, and GR 17/2025 further emphasizes that this consent must be clear, explicit, and responsible. According to Article 7, par (1) of GR 17/2025, electronic service operators must obtain the consent of a parent or legal guardian to process the personal data of children and adolescents.

8. Japan

The APPI Guidelines state that, with regard to the consent of the individual specified in the APPI, if a minor does not have the capacity to judge the consequences of consenting to the handling of personal data, consent must be obtained from a parent or other guardian.

9. Republic of Korea

To process personal data of minors under 14 years of age, the consent of their legal guardian is required.

10. Malaysia

Under sub regulation 3 of the Personal Data Protection Regulation 2013, a data controller must obtain consent from the parent, guardian, or person with parental responsibility for minors under 18 years old. This ensures the processing of children's or adolescents' personal data is done only with proper approval from those responsible for their welfare.

11. Mexico

Consent is a necessary element for the processing of personal data, which only is granted, by the parents or legal guardians of the children or adolescents.

12. New Zealand

Not applicable as there is no distinction in relation to the legal bases available for the processing of children's and adolescents' personal data and those applicable for adults. An authorization (consent) from a legal representative is exceptionally recognized as a legal basis for collecting, using, and disclosing personal data of minors.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

No information was found in relation to this issue. However, although personal data protection laws contain provisions on the protection of children's personal data, it does not explicitly require parental consent or stipulate separate legal grounds for processing children's personal data.

15. The Republic of the Philippines

No information was found in relation to this issue.

16. The Russian Federation

The consent of a parent or legal guardian is required.

17. Singapore

Where an organization has reason to believe that a child does not have sufficient understanding of the nature and consequences of giving consent, the organization should obtain consent from the child’s parent or guardian.

18. Chinese Taipei

The consent of a person with parental responsibility is recognized as a separate legal basis for processing.

19. Thailand

For children under 10, the consent of a legal guardian is mandatory. For competent minors between 10 and 20, their own consent is sufficient.

20. United States

Verifiable parental consent is considered a valid, primary legal basis for children under 13.

21. Viet Nam

According to Decree No. 13/ND-CP, the processing of children’s personal data requires the consent of the child if the child is 7 years of age or older, along with the consent of the parent or legal guardian as prescribed. Entities authorized to process such data must verify the child’s age prior to processing their personal data.

III. Comparative Analysis and Implications

The following table indicates whether the consent of a legal representative is recognized as a valid legal basis for processing a child's data when the child cannot provide valid consent on their own.

Table 12 Recognized Legal Bases for Processing Children's and Adolescents' Personal Data

APEC Economy	Is Consent from a Legal Representative a Recognized Legal Basis? (O/X)
Australia	O
Brunei Darussalam	N/A (No information was found in relation to this issue)
Canada	N/A (No information was found in relation to this issue)
Chile	O
People's Republic of China	O
Hong Kong, China	O
Indonesia	O
Japan	O
Republic of Korea	O
Malaysia	O
Mexico	O
New Zealand	N/A
Papua New Guinea	N/A (No information was found in relation to this issue)
Peru	N/A (No information was found in relation to this issue)
The Republic of the Philippines	O
The Russian Federation	O
Singapore	O
Chinese Taipei	O
Thailand	O
United States	O
Viet Nam	O

The comparative analysis reveals a near-universal consensus across APEC economies regarding the legal basis for processing the personal data of children and adolescents who lack the capacity to provide valid consent. In every economy for which information is available, the consent of a legal representative, most commonly a parent or guardian, is recognized as the primary and lawful basis for such processing. This reflects the consistent application of a long-standing legal principle whereby responsibility for children and adolescents' welfare and decision-making is entrusted to a legally authorized adult.

This establishes a clear baseline rule for children and adolescents' data protection within the APEC region. Regardless of differences in broader data protection frameworks, the reliance on proxy consent functions as a foundational safeguard, compensating for their limited capacity to understand the implications of data processing. In some jurisdictions, this model is further refined through age thresholds or dual-consent requirements that combine the assent with parental authorization, particularly for older children or adolescents. Nevertheless, the core principle remains stable: where a child and adolescent cannot validly consent, processing must be grounded in the consent of a legal representative.

From a compliance and governance perspective, these findings carry significant implications for organizations operating across multiple APEC economies. Any service that processes children's or adolescents' personal data must implement robust mechanisms to obtain, verify,

and manage parental or guardian consent. Reliance solely on consent is legally insufficient in nearly all jurisdictions and presents substantial compliance risk. While subsequent sections demonstrate divergence in the operational details of proxy consent, such as verification methods, age thresholds, and authorized parties, the underlying consensus provides a clear compliance anchor for designing child-centered data protection frameworks.

Section 3 Scope of Consenting Parties

I. Introduction

The integrity of consent as a protective measure is contingent upon the authority and accountability of the party providing it. This inquiry is critical for defining the precise scope of who is empowered to consent on a child's behalf. Legal frameworks traditionally designate the legal representative (e.g., a parent or guardian) as the primary authority, based on their legal duty to act in the child's best interest. However, different contexts may call for different approaches. For instance, in an educational setting, a school official might be positioned to provide informed consent for a specific academic service. Conversely, a legal representative may not always possess the technical expertise to fully grasp the data processing implications or may have their own interests to consider. Therefore, examining which parties are permitted to consent helps assess how a legal system balances the general duty of a parent with the contextual relevance of other figures. This allows for an evaluation of where accountability is placed and how the risks of uninformed decisions or potential conflicts of interest are managed across all possible consenting parties.

II. Status of APEC economies

1. Australia

OAIC guidance provides that if an entity is unsure if an individual has the capacity to give consent at a particular time, it should consider offering support, such as an interpreter. If such support is insufficient, the entity may consider if someone can act on the individual’s behalf, such as a guardian, someone with enduring power of attorney, a person recognized by other relevant laws, or a person the individual nominated in writing when they were capable of giving consent.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

Pursuant to guidance provided by the OPC under PIPEDA, only parents or legal guardians are authorized to consent on behalf of minors who lack the capacity for meaningful consent

themselves. In such cases, consent for a child's personal data must be given by a parent or legal guardian, or another person who holds formal legal authority over the child.

4. Chile

Consent is limited to parents and legal guardians.

5. People's Republic of China

The parents or other guardians of the minors.

6. Hong Kong, China

A person who has parental responsibility for the minor could give the prescribed consent on behalf of the minor.

7. Indonesia

No information was found in relation to this issue.

8. Japan

Persons who act on behalf of minors to give consent are not limited to parents with parental authority.

9. Republic of Korea

The PIPA limits the consenting party for the processing of a child's personal data to their legal guardian (including guardians under the Civil Act).

10. Malaysia

According to sub regulation 3 of the Personal Data Protection Regulation 2013, only the parent, legal guardian, or person with parental responsibility can provide consent for the processing of a minor's personal data.

11. Mexico

The ability to grant consent for the processing of children's and adolescents' personal data is limited exclusively to the parents or legal guardians of the child or adolescent, following the relevant provisions of the Mexican civil law.

12. New Zealand

A representative isn't just restricted to a child's parents or legal guardian. A representative is a person who is exercising the child's privacy rights on their behalf. For example, if it is determined that the parent is not acting in the best interests of the child, they will not be considered the child's representative and will not be able to exercise the child's rights on the child's behalf.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

No information was found in relation to this issue.

15. The Republic of the Philippines

When the consent is required for processing of minor's personal data, it would be the parent/s or legal guardian who would give consent on behalf of the minor.

16. The Russian Federation

The consenting party is limited to the parent or guardian.

17. Singapore

Where the child is below 13 years of age, the organization must obtain consent from the child's parent or guardian.

18. Chinese Taipei

Limited to persons with parental responsibility.

19. Thailand

The consenting party is the parent or guardian, and in some cases the minor themselves.

20. United States

Parents/legal guardians provide consent. There is some discussion in response to public comments by the FTC on a previous version of COPPA that contemplates the potential role of schools as able to consent on behalf of parents. Neither COPPA nor the COPPA rule, however, concludes that schools may automatically or by operation of law, consent on behalf of parents under those laws as part of an agency relationship.

21. Viet Nam

According to Decree No. 13/ND-CP, the processing of children's personal data requires the consent of the child if the child is 7 years of age or older, along with the consent of the parent or legal guardian as prescribed.

III. Comparative Analysis and Implications

The following table indicates whether the authority to consent on behalf of a minor is strictly limited to legal representatives (e.g., parents, guardians) or if it can be extended to other parties (e.g., school officials) in specific contexts.

Table 13 Scope of Consenting Parties

APEC Economy	Is the Consenting Party Limited to a Legal Representative? (O/X)
Australia	X
Brunei Darussalam	No information was found in relation to this issue
Canada	O
Chile	O
People's Republic of China	O
Hong Kong, China	O
Indonesia	No information was found in relation to this issue
Japan	X
Republic of Korea	O
Malaysia	O
Mexico	O
New Zealand	X
Papua New Guinea	No information was found in relation to this issue
Peru	No information was found in relation to this issue
The Republic of the Philippines	O
The Russian Federation	O
Singapore	O
Chinese Taipei	O
Thailand	O
United States	X
Viet Nam	O

The comparative analysis shows that a majority of APEC economies adopt a strict and formal approach to the scope of parties authorized to consent on behalf of a child and adolescent, limiting such authority exclusively to parents or legal guardians. This model reflects a strong emphasis on legal certainty and accountability, grounded in the traditional duty of care imposed on legal representatives. By designating a single, clearly defined consenting authority, these frameworks aim to minimize ambiguity, reduce the risk of invalid consent, and simplify compliance for data controllers.

However, a minority of economies permit a more flexible and context-dependent allocation of consent authority. In some jurisdictions, legal frameworks allow parties other than parents or guardians, such as schools or other representatives acting in the child's best interests, to provide consent in specific circumstances. These approaches recognize that parents or guardians may not always be best positioned to evaluate the implications of particular data processing activities, especially in institutional or educational contexts, and seek to align consent authority with contextual expertise and functional responsibility. Or they recognize that parents can sometimes authorize others to provide consent on their behalf.

This divergence has significant implications for cross-border compliance and risk management. International service providers cannot rely on a uniform proxy-consent model and must instead design consent mechanisms that are sensitive to jurisdiction-specific rules governing who may lawfully consent on a child's and adolescent's behalf. Failure to properly identify and authenticate the authorized consenting party may invalidate the legal basis for processing and expose organizations to regulatory and enforcement risks. At the same time, flexible models shift compliance from a purely formal exercise to a substantive evaluation of authority, accountability, and context regarding the needs of children and adolescents. These findings underscore the need for adaptable consent frameworks capable of accommodating both strict representative-based models and more functional, context-driven approaches within the APEC region.

Section 4 Scope of Minors' Independent Consent

I. Introduction

This question addresses the principle of "evolving capacities." Minors are not a homogeneous group; their ability to understand and make decisions grows with age. A legal framework's approach to this issue reveals how it balances the need for protection with the recognition of a minor's growing autonomy. Defining the age or circumstances under which a minor can provide their own valid consent is a key policy decision that reflects a nuanced understanding of child development, ensuring that rules are appropriately tailored rather than overly restrictive for older adolescents.

II. Status of APEC economies

1. Australia

Entities must decide on a case-by-case basis whether an individual under the age of 18 has the capacity to consent. The OAIC has advised that as a general rule: an individual under the age of 18 has the capacity to consent if they have the maturity to understand what is being proposed, if it is not practical to assess the capacity of individuals on a case-by-case basis, an entity may assume an individual over the age of 15 has capacity, unless they are unsure.

2. Brunei Darussalam

It appears that there is no differentiation based on the age of the data subject for the processing of personal data of children and adolescents in Brunei Darussalam. All data subjects seem to be able to exercise their consent rights equally.

3. Canada

Pursuant to guidance provided by the OPC under PIPEDA, children and adolescents can independently provide valid consent for the collection, use, or disclosure of their personal data only if they have the capacity to understand the nature, purpose, and consequences of that consent.

4. Chile

Minors aged 16 and 17 can independently consent to the processing of non-sensitive personal data, or sensitive personal data.

5. People's Republic of China

Minors aged 14 and over are considered mature enough to understand the implications of personal data processing and can consent independently.

6. Hong Kong, China

Parental consent is required for all minors under 18.

7. Indonesia

No information was found in relation to this issue.

8. Japan

No information was found in relation to this issue.

9. Republic of Korea

According to the PIPA, a child under 14 years of age is not permitted to provide consent independently without the involvement of their legal guardian. However, individuals aged 14 years or older can provide consent independently.

10. Malaysia

In Malaysia, children or adolescents under 18 cannot independently provide valid consent for the processing of their personal data. Parental consent is required for all minors under 18.

11. Mexico

Children and adolescents cannot generally provide valid, independent consent for the processing of their personal data without the involvement of a legal guardian. Consent must come from a parent or legal representative when the data subject is underage, these representation rules, are established among the Mexican civil law.

12. New Zealand

In New Zealand privacy law, there is no defined age where a child or young person can provide valid authorization (consent). An assessment is made by the agency as to whether the child or adolescent can understand what they are consenting to, and any potential consequences of providing that authorization.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

No information was found in relation to this issue.

15. The Republic of the Philippines

No information was found in relation to this issue.

16. The Russian Federation

According to the Civil Code, children aged 14 and over can independently consent in certain areas, such as managing their own income or copyright earnings (small transactions).

17. Singapore

The PDPC considers that a minor between 13 and 20 years old may give valid consent, when the policies on the collection, use and disclosure of the minor's personal data, as well as the withdrawal of consent, are readily understandable by them. This includes ensuring that the minor understand the consequences of providing and withdrawing consent. However, where an organization has reason to believe that a minor does not have sufficient understanding of the nature and consequences of giving consent, the organization should obtain consent from the minor’s parent or guardian.

18. Chinese Taipei

No information was found in relation to this issue.

19. Thailand

Minors aged 10-20 can independently consent for acts deemed competent under the Civil and Commercial Code.

20. United States

Under the COPPA, children under 13 cannot consent. However, some states set the age of consent higher.

21. Viet Nam

Children and adolescents cannot independently provide valid consent without the involvement of a parent or legal guardian.

III. Comparative Analysis and Implications

The following table indicates whether minors can provide valid, independent consent for the processing of their personal data without the involvement of a legal representative, often dependent on an age threshold or a capacity assessment.

Table 14 Scope of Minors' Independent Consent

APEC Economy	Can a Minor Provide Independent Consent? (O/X)
Australia	O (Case-by-case, generally 15+)
Brunei Darussalam	O (No differentiation)
Canada	O (If they have capacity)
Chile	O (16+)
People’s Republic of China	O (Generally 14+, with exceptions)
Hong Kong, China	O
Indonesia	N/A (No information was found in relation to this issue)
Japan	N/A (No information was found in relation to this issue)
Republic of Korea	O (14+)
Malaysia	X (Not under 18)
Mexico	X
New Zealand	O (If they have capacity)
Papua New Guinea	N/A (No information was found in relation to this issue)
Peru	N/A (No information was found in relation to this issue)
The Republic of the Philippines	N/A (No information was found in relation to this issue)
The Russian Federation	O (14+, for small transactions)
Singapore	O (13+)
Chinese Taipei	N/A (No information was found in relation to this issue)
Thailand	O (10+, for competent acts)
United States	O (Generally 13+)
Viet Nam	X

The APEC economies are highly divided on the issue of a minor's capacity for independent consent, reflecting differing legal and cultural views on child autonomy. One group, including Malaysia; Mexico; and Viet Nam, adopts a protective stance, requiring parental consent for all minors until they reach the age of majority. This approach prioritizes protection over the minor's evolving capacity.

A second group establishes a clear, fixed age threshold at which a minor is presumed capable of providing their own consent. This age varies significantly, from 13 in Singapore, to 14 in China and Korea, and 16 in Chile. A third group, including Australia; Canada; and New Zealand, eschews a fixed age in favor of a flexible, case-by-case assessment of an individual minor's capacity to understand the consequences of their consent.

This fragmentation requires businesses to adopt a highly differentiated compliance strategy. A service cannot apply a single age gate across the APEC economies. To comply, companies must implement systems capable of adapting to different age thresholds and, in some economies, be prepared to make reasonable, case-by-case assessments of a minor's capacity. This complexity underscores the importance of a nuanced approach that respects both the need for protection and the principle of a minor's evolving autonomy.

Section 5 Regulation of Consent Verification Methods

I. Introduction

A legal requirement for parental consent is only effective if it is practically enforceable. This question is vital because it examines whether the law moves from theory to reality by mandating concrete, verifiable consent mechanisms. Without such rules, a consent requirement can be easily circumvented (e.g., by a child simply ticking a box). Inquiring into the existence and specifics of these verification methods allows for an assessment of the technical and procedural robustness of the framework, ensuring that the protection is real and not merely symbolic.

II. Status of APEC economies

1. Australia

No information was found in relation to this issue.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

PIPEDA does not prescribe specific anti-impersonation measures, but organizations are expected to adopt reasonable steps, proportionate to the privacy risks, to verify that guardian consent is authentic.

4. Chile

No information was found in relation to this issue.

5. People's Republic of China

There appears to be no specific regulation.

6. Hong Kong, China

No information was found in relation to this issue.

7. Indonesia

No information was found in relation to this issue.

8. Japan

Under the APPI, there are no provisions regarding measures to prevent minors from impersonating their own legal representatives.

9. Republic of Korea

Article 17-2, Paragraph 1 of the Enforcement Decree of the PIPA stipulates specific methods for confirming whether there is a valid consent. These methods include:

- Notifying the legal guardian via a mobile phone message that the data controller has confirmed the consent;
- Receiving credit card, debit card, or other card information from the legal guardian;
- Verifying the identity of the legal guardian through mobile phone authentication or similar means;
- Issuing a written consent form to the legal guardian or sending it by mail or fax, which the legal guardian then signs and submits;
- Sending consent confirmation via email;
- Confirming consent through a telephone call;
- Other equivalent methods.

10. Malaysia

To prevent impersonation of a legal guardian, data controllers are required to implement verification measures. This may include email verification, two-factor authentication, or documentary verification of guardianship to ensure that consent is being provided by the

legitimate guardian of the minor. These measures protect against fraudulent consent and ensure compliance with the regulations.

11. Mexico

As established by the laws of both the public and private sector, the rules for the representation of underage data subjects shall be carried out, in accordance with the relevant provisions of the Mexican civil law. In this regard, the Mexican civil law, establishes an obligation to verify the identity of every party in a procedure by verifying an official identity document, this obligation is applicable for data controllers when obtaining consent. Additionally, the provisions derived from the data protection laws, establish that for the accreditation of underage data subject's identity, as well as the character of the parents or legal guardians, when exercising ARCO rights, the following documents must be presented: Birth certificate of the child or adolescent, Legal documents that demonstrate the legal representation of the child or adolescent, Official identification of the adult exercising the legal representation of the child or adolescent. These provisions are also applicable for demonstrating the identity of an underage data subject and the legal representation of their parents, and legal guardian when granting consent for a data processing.

12. New Zealand

Where a parent is determined to be acting as the representative of the child for the purposes of exercising the child's right to access or correct their personal data, an agency must ensure, through the adoption of appropriate measures, that the information intended for the recipient is received only by that intended recipient. In practice, most agencies will request identification documentation and other documentation to verify that the requestor is who they say they are.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

No information was found in relation to this issue.

15. The Republic of the Philippines

No information was found in relation to this issue.

16. The Russian Federation

No information was found in relation to this issue.

17. Singapore

The PDPA does not prescribe specific measures for organizations to prevent impersonation of legal guardians. Section 14(4) of the PDPA provides that consent given or deemed to have been given by an individual for the collection, use, or disclosure of the individual's personal data, includes consent given or deemed to have been given by any person validly acting on behalf of that individual for the collection, use, or disclosure of the personal data.

18. Chinese Taipei

No information was found in relation to this issue.

19. Thailand

No information was found in relation to this issue.

20. United States

Under COPPA, "verifiable parental consent" requires methods reasonably calculated, in light of technology, to ensure the person providing consent is the child's parent:

Methods per COPPA, 16 CFR Part 312.5: government ID upload (excluding retention), signature on a consent form, or similar, not just by email.

The FTC has sanctioned companies for inadequate verification, e.g., easily bypassed email-only methods.

21. Viet Nam

There are currently no provisions regarding measures to prevent impersonation.

III. Comparative Analysis and Implications

The following table indicates whether an economy's laws or regulations mandate specific methods to verify that the person providing consent on behalf of a child is indeed their legal representative.

Table 15 Regulation of Consent Verification Methods

APEC Economy	Are There Specific Regulations for Verifying Guardian Consent? (O/X)
Australia	X
Brunei Darussalam	N/A (No information was found in relation to this issue)
Canada	O (reasonable verification steps expected)
Chile	N/A (No information was found in relation to this issue)
People's Republic of China	X
Hong Kong, China	N/A (No information was found in relation to this issue)

Indonesia	N/A (No information was found in relation to this issue)
Japan	X
Republic of Korea	O
Malaysia	O
Mexico	O
New Zealand	X (Appropriate measures expected)
Papua New Guinea	N/A (No information was found in relation to this issue)
Peru	N/A (No information was found in relation to this issue)
The Republic of the Philippines	X
The Russian Federation	N/A (No information was found in relation to this issue)
Singapore	X (No explicit rule, but organizations must verify someone validly acts on behalf)
Chinese Taipei	N/A (No information was found in relation to this issue)
Thailand	N/A (No information was found in relation to this issue)
United States	O (COPPA specifies detailed methods for verifying parental consent)
Viet Nam	X

There is a stark divide among APEC economies regarding the enforcement of parental consent. A majority of jurisdictions do not legally prescribe specific technical or procedural methods for verifying the identity of a legal guardian. While they may require "reasonable" or "appropriate" steps, the absence of concrete rules leaves significant discretion to companies and can render consent requirements symbolic rather than practical, as they can be easily circumvented by a child.

In sharp contrast, a small group of economies—notably Korea; Mexico; and the United States—have moved from theory to practice by mandating specific, verifiable consent mechanisms. The United States COPPA Rule lists acceptable methods like using a government ID or a signed consent form, expressly moving beyond easily faked email confirmations. Korea's PIPA details numerous options, including mobile phone authentication and credit card verification. Mexico requires verification against official identity documents as per its civil law.

This gap between principle and enforcement is a critical point of weakness in many child protection frameworks. For companies, the implication is twofold. In economies like Korea and the United States, compliance requires implementing specific, often costly, technical solutions. In economies without such rules, relying on simple, unverified methods carries a significant reputational and potential legal risk, as regulators could still deem such practices "unreasonable." The trend set by Korea and the United States suggests that expectations for robust verification are likely to increase globally.

Section 6 Permissibility of Bundled (Comprehensive) Consent

I. Introduction

This question addresses the core data protection principles of specific, granular, and informed consent. For a vulnerable group like children, this is paramount. Allowing a data

controller to obtain broad, "bundled" consent for all processing activities upfront would undermine the protective framework. It prevents the legal representative from making a truly informed decision about the distinct risks and benefits of each processing purpose. Determining whether the law prohibits this practice is essential to verify that consent remains a meaningful, deliberate choice for each specific activity, rather than a one-time, all-encompassing waiver of a child's privacy rights.

II. Status of APEC economies

1. Australia

Consent must be current and specific. This means that consent cannot be assumed to apply indefinitely, or for purposes that are broader than the specific purpose for which it was sought.

2. Brunei Darussalam

The Personal Data Protection Order (PDPO) is not yet in force. However, it requires an informed consent, which implicitly restricts the validity of broad, bundled consent that fails to clearly specify purposes.

3. Canada

Blanket or comprehensive consent for all data processing activities, especially for children or adolescents is not valid under PIPEDA. Consent must be informed, specific, and meaningful for each purpose contemplated.

4. Chile

No information was found in relation to this issue.

5. People’s Republic of China

The PIPL requires 'Separate Consent’ for processing sensitive personal information (which includes minors' data) and for transferring data to third parties.

6. Hong Kong, China

No specific prohibition against bundled consent was found.

7. Indonesia

The GR 17/2025 requires data processing to be based on "legitimate and explicit purposes." This principle limits the scope of any blanket consent, effectively requiring purpose-specific consent.

8. Japan

It is not permissible for a business operator handling personal data to obtain blanket prior consent, regardless of whether the personal data pertains to children or young persons. They are required to obtain appropriate consent for the handling of such data in accordance with the APPI.

9. Republic of Korea

Obtaining comprehensive prior consent for the overall processing of children and adolescents' personal data is not permitted. According to Article 22 of the PIPA, consent must be obtained separately for each specific purpose or item.

10. Malaysia

Data controller can obtain comprehensive, prior consent for all personal data processing activities involving children or adolescents. This consent must come from a parent or legal guardian.

11. Mexico

Under Mexican law, it is not permissible for the data controller, whether in the private or public sector, to obtain comprehensive, prior consent for all personal data processing activities involving children or adolescents. In the private sector, the LFPDPPP mandates that processing personal data of minors must be based on the informed and specific consent of their legal representatives, such as parents or guardians. Consent that is broad or generalized—without clearly identifying the purposes and scope of processing—does not meet the legal standards of validity and transparency established by this law. Similarly, in the public sector, the LGPDPPSO imposes strict safeguards. Article 7 of this law explicitly states that in the processing of minors' personal data, the best interest of the child or adolescent must be prioritized in accordance with applicable legal provisions. This means that beyond obtaining consent from legal guardians, any data processing involving minors must adhere strictly to the principles of necessity, proportionality, and be aimed at promoting or protecting the minor's well-being. In both legal frameworks, the principles of purpose limitation, proportionality, and informed consent are central. Therefore, obtaining broad or blanket consent for unspecified future uses of minors' data is inconsistent with Mexican data protection laws and may result in non-compliance.

12. New Zealand

As the Privacy Act is principle based, rather than consent based, the agency wanting to collect, use or share a child or young person's personal data, must comply with the Information Privacy Principles, which may or may not involve obtaining authorization (consent) from the child or young person or another person providing consent on their behalf. Where an agency wants to use a child or young person's personal data for another purpose to that for which it was collected, the agency must have legal authority that enables

that secondary use (which may or may not involve obtaining consent from the child or young person, or another person providing consent on their behalf.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

Peru's Personal Data Protection Law requires consent to be "free, prior, informed, express, and unequivocal." This high standard generally rules out bundled consent for unspecified or diverse purposes, especially for minors.

15. The Republic of the Philippines

Consent obtained should be limited to the specific and declared purposes of the processing of personal data.

16. The Russian Federation

The law requires consent to be "specific, informed, and conscious." While not explicitly prohibiting bundled consent, the requirement for specificity makes obtaining a single, broad consent legally risky and potentially invalid.

17. Singapore

Comprehensive prior consent is not permitted, as the organizations must ensure that they do not collect, use or disclose more personal data than is reasonably necessary in order to achieve the purpose.

18. Chinese Taipei

The consent must be "informed" and "explicit," and it must be for a "specific purpose." This principle generally prohibits blanket or bundled consent for multiple, distinct purposes.

19. Thailand

Comprehensive prior consent is not permitted; separate consent is required for each purpose and activity.

20. United States

COPPA prohibits blanket, open-ended parental consent. Operators must give specific, clear notice about (a) what data will be collected, (b) how it will be used, and (c) to whom it will be disclosed. Operators must also obtain new consent if practices change materially.

21. Viet Nam

The law requires data processing to adhere to the principle of "purpose limitation," and consent must be "voluntary and informed." These principles make broad, bundled consent inconsistent with the legal framework.

III. Comparative Analysis and Implications

The following table indicates whether data controllers are permitted to obtain a single, "bundled" or comprehensive consent for all data processing activities involving a minor, or if separate, granular consent is required for each purpose.

Table 16 Permissibility of Bundled (Comprehensive) Consent

APEC Economy	Is Bundled Consent Permitted for Minors' Data? (O/X)
Australia	X
Brunei Darussalam	X
Canada	X
Chile	-
People’s Republic of China	X
Hong Kong, China	-
Indonesia	X
Japan	X
Republic of Korea	X
Malaysia	O
Mexico	X
New Zealand	X (Principles-based, not consent-based)
Papua New Guinea	-
Peru	X
The Republic of the Philippines	X
The Russian Federation	X
Singapore	X
Chinese Taipei	X
Thailand	X
United States	X
Viet Nam	X

The majority of APEC economies prohibit the practice of obtaining bundled, all-encompassing consent for processing children's personal data. Economies like Canada; Korea; Thailand; and the United States mandate that consent must be specific, granular, and obtained for each distinct processing purpose. This approach aligns with the core data protection principle that consent must be truly informed, which is impossible if a guardian is asked to agree to a wide range of current and future data uses with a single action. However, there are critical exceptions. Malaysia explicitly permits data controllers to obtain comprehensive, prior consent for all processing activities, provided it comes from a legal

guardian and is properly recorded. This places a significant burden on the guardian to understand all potential implications upfront and diverges sharply from the global trend toward granularity. While China's law does not permit it, corporate practice suggests bundled consent is a common method for user registration.

This distinction highlights a fundamental difference in how "informed consent" is interpreted. For companies, the prevailing standard across APEC requires designing user interfaces and privacy flows that allow guardians to make separate choices about different data processing activities. Relying on a single checkbox to gain broad consent is non-compliant and legally risky in most of the APEC economies.

The core implication is that a regulatory action could help solidify this trend. The current framework's effectiveness relies too heavily on corporate adherence to "prevailing standards," which may not be consistently enforced. APEC economies may therefore consider adopting a clear, statutory prohibition on bundled consent for minors, ensuring that a refusal to consent to non-essential data processing does not penalize the child by denying them access to the primary service.

Chapter 6 Clear and Understandable Notice to Children or Adolescents

The principle of transparency is fundamental to data protection, but it is only meaningful if the notice is understood by the recipient. For children and adolescents, whose comprehension skills are still developing, standard privacy policies or notices designed for adults often fail to provide genuine understanding. This can prevent them from exercising their rights effectively. Therefore, mandating notices that are provided in clear, plain, and age-appropriate language is a crucial element for guaranteeing their right to know and enabling substantive data protection. This chapter aims to understand how different economies across APEC are implementing this vital principle.

Section 1 Legal distinctions between adults and minors

I. Introduction

This inquiry is critical to determine whether a legal framework moves beyond passive transparency to mandate active, age-appropriate communication. Establishing whether easy-to-understand notices are a legal obligation is the first step in assessing a system's commitment to effective communication with minors. The second part of the question—regarding specific requirements in laws or guidelines (e.g., use of illustrations, plain language, or videos)—is equally vital. It allows for an evaluation of whether the law provides concrete, actionable standards for compliance, or if it leaves the obligation vaguely defined, which could lead to inconsistent and ineffective implementation.

II. Status of APEC economies

1. Australia

There is no legal obligation specifically in relation to children or adolescents. Under Australian Privacy Principle (APP) 1, entities must have a clearly expressed and up to date privacy policy about their management of personal data. APP 1.4 outlines the types of information that privacy policies must contain. The Children’s Online Privacy Code (currently being developed), may provide further specification on how existing requirements are to be complied with, with respect to children.

2. Brunei Darussalam

The Personal Data Protection Order (PDPO) is not yet in force, and no specific requirement for child-friendly notices is confirmed in the legislation.

3. Canada

Pursuant to guidance provided by the OPC under PIPEDA, organizations have a legal obligation to ensure that privacy notices and consent requests are presented in a manner that is easy for children or adolescents to understand, if their personal data is being collected, used, or disclosed. This obligation arises from the requirement that consent must be meaningful for all individuals, including minors. PIPEDA (Section 6.1): Consent must be "reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal data...".

4. Chile

When events like a data breach occur, the data controller must notify of the incident in a clear and simple manner.

5. People’s Republic of China

Article 9 of the Regulations on the Network Protection of Children's Personal data stipulates that when network operators seek consent from children's guardians for the collection, use, transfer, or disclosure of children's personal data, they must provide notice in a clear and prominent manner.

6. Hong Kong, China

No specific formats or language for privacy notices in respect of children/adolescents. Under the PDPO, the general obligation for data users is to take all reasonably practicable steps to inform the data subjects of information such as the purpose for which personal data is to be used and the classes of persons to whom the data may be transferred.

7. Indonesia

GR 17/2025 emphasizes that online service information must be delivered in a way that is easily understandable for children's respective age groups. For instance, short, simple videos or illustrations can be used to explain safe usage methods. The regulation also states that children have the right to know if they are being monitored online. If a service allows parents, guardians, or other users to monitor a child's activity or location, the system must inform the child of this monitoring through clear and prominent notifications (symbols, warnings, pop-ups, etc.). This enhances transparency and explicitly prohibits secret or undisclosed monitoring. Additionally, the regulation requires the provision of tools for children and their parents/guardians to easily exercise their rights or file complaints about the service. For example, a 'mute word' feature should be available to block specific words, phrases, hashtags, or usernames from feeds, searches, and notifications. Such tools must be easily accessible and come with clear instructions on how to use them. In case of issues, a prompt response and appropriate resolution measures must be taken.

8. Japan

Under the APPI, there are no explicit provisions that mandate providing privacy notices in a manner that is easy for minors to understand. However, a business operator handling

personal data must, when obtaining consent from the individual or notifying or making public the purpose of use, do so by reasonable and appropriate methods according to the nature of the business and the handling of personal data.

9. Republic of Korea

According to Article 22-2, Paragraph 3 of the PIPA, when a data controller provides notifications or similar communications related to personal data processing to a child under 14 years of age, they must use an easy-to-understand format and clear, simple language. Furthermore, PIPC through its "Guide to Personal Data Protection for Children and Adolescents," recommends that not only for children under 14, but also for minors aged 14 to under 18, support should be provided to help data subjects make their own decisions regarding personal data matters, using language, pictures, and videos that are easy for them to understand.

10. Malaysia

No specific obligation was found.

11. Mexico

There is a legal obligation to ensure that privacy notices addressed to children or adolescents are understandable for them, but the laws do not mandate specific formats (e.g., illustrations or icons). Instead, they impose general duties to favor clarity and comprehensibility based on the audience’s characteristics.

12. New Zealand

There is no specific obligation to provide a privacy notice in a manner that is easy for children and young people to understand. However, this requirement is implicit within the notification requirements of Information Privacy Principles 3 and 4. Under Information Privacy Principle 3, an agency must take reasonable steps to ensure an individual is aware of certain matters relating to a collection. Where an agency is collecting information directly from children or young people, this requirement means the agency has to ensure the notification is made in a way that the child or young person will understand. Further, Information Privacy Principle 4 requires that the way an agency collects information is fair. As such, if a child or young person does not understand why their personal data is being collected and what the agency is going to do with that information, the manner of collection could be considered unfair.

13. Papua New Guinea

No specific obligation was found.

14. Peru

No information was found in relation to this issue.

15. The Republic of the Philippines

Under the DPA, organizations must ensure that any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language. The Advisory on Guidelines on Child-Oriented Transparency states that organizations must ensure that children are aware of the nature, purpose, and extent of the processing of personal data. They should consider the readability (e.g., vocabulary, tone, or style), comprehension, and granularity of Privacy Notices while taking into consideration the best interests and evolving capacities of children. Organizations shall also ensure that the Privacy Notice, including any information and communication relating to the processing of personal data, is readily accessible, taking into consideration user experience and user interface. They must clearly inform children how to access any information or communication relating to the processing of their personal data. Organizations may utilize a variety of alternative formats, such as videos, infographics, animations, and audio recordings, to deliver privacy-related information to children. They should design these formats to ensure that the Privacy Notices are presented in a manner that is simple and easily understandable, taking into consideration the age range of the intended or likely users. (Section 3).

16. The Russian Federation

Federal Law No.152-FZ does not mandate child-friendly notices. However, Federal Law 436-FZ regulates age rating labels and warnings for harmful information.

17. Singapore

The PDPC recognizes that children are unique individuals with varying developmental abilities. While there is no one-size-fits-all approach when communicating with individuals within this age bracket, organizations should consider the nature of their content and adopt age-appropriate language and media (e.g. infographics, video clips). When communicating with children, organizations must use language that is readily understandable by children so that children may understand the consequences of providing and withdrawing consent. This means that the notification of purpose and consent clauses, data protection policies, and terms and conditions, must be in language that is readily understandable by children.

18. Chinese Taipei

No such obligation exists.

19. Thailand

The PDPA and PDPC guidelines require notices to be in easy-to-understand language and format; the notice must be clearly separate and easy for the consumer to comprehend.

20. United States

COPPA requires “clear and prominent” notice “in language understandable by the parents.” FTC staff guidance encourages using visuals, accessible language, and layered notices.

21. Viet Nam

Article 7 of Decree No. 13/ND-CP stipulates: “Individuals have the right to be informed and notified about the processing of their personal data,” which includes children’s right to be informed and notified. However, there are currently no specific guidelines on the format or child-friendly language to be used for this purpose.

III. Comparative Analysis and Implications

The following table indicates whether there is a specific legal obligation for privacy notices to be presented in a clear, plain, and age-appropriate format that is easily understandable by children and adolescents.

Table 17 Legal distinctions between adults and minors

APEC Economy	Legal Obligation for Age-Appropriate Notices? (O/X)
Australia	X (But a code is in development)
Brunei Darussalam	X
Canada	O
Chile	O (For data breach notifications)
People’s Republic of China	O
Hong Kong, China	X
Indonesia	O
Japan	X
Republic of Korea	O
Malaysia	X
Mexico	O (But no specific formats mandated)
New Zealand	X (Implicitly required)
Papua New Guinea	X
Peru	-
The Republic of the Philippines	O
The Russian Federation	X
Singapore	O
Chinese Taipei	X
Thailand	O
United States	O (Notice to parents, not children)
Viet Nam	X (General right to be informed, no specific format)

A clear trend is emerging across APEC to move beyond passive transparency toward mandated, age-appropriate communication. A significant number of economies, including Canada; China; Indonesia; Korea; and the Philippines, have established explicit legal obligations requiring that privacy notices for children be provided in an easy-to-understand

format using clear and simple language. Some jurisdictions, such as Indonesia and the Philippines, offer even more concrete guidance. Indonesia explicitly suggests using short, simple videos or illustrations and mandates clear, prominent notifications for monitoring. The Philippines' Advisory similarly suggests utilizing videos, infographics, animations, and layered notices to enhance comprehension, reflecting a design standard that centers on the "best interests and evolving capacities of children."

However, several economies still lack such specific mandates. While they may have general transparency requirements, they do not explicitly require that notices be adapted for a younger audience. Crucially, the analysis shows that the general data protection principles of 'fairness' and 'informed consent' may create a strong implicit legal obligation in several jurisdictions, even without specific formatting rules. This demonstrates that legal risk is present even in economies marked 'X' if the standard notice is demonstrably incomprehensible to a minor.

The primary implication for businesses is that standard, text-heavy privacy policies designed for adults are no longer sufficient for services accessed by minors in many APEC economies. As regulatory expectations shift toward user-centric designs that actively facilitate understanding, companies should consider proactively adopting best practices—such as layered notices, dashboards, and icons—not only to ensure compliance but also to build trust in markets where such rules are not yet explicit. This corporate shift, however, would benefit from a more robust regulatory framework. Therefore, APEC economies should consider issuing detailed standards that guide companies in implementing these strategies, rather than relying on vague recommendations. By noting importance of comprehension testing with children’s focus groups and establishing that a failure to provide age-appropriate notice is equivalent to a failure to obtain valid consent, regulators can more effectively reinforce the legal obligation to communicate clearly.

Section 2 Analysis of Corporate Practices and Case Studies

I. Introduction

While legal mandates set the minimum standard, actual industry practice reveals the true state of data protection on the ground. This question is important for two key reasons. First, in economies without a strict legal mandate, identifying voluntary adoption by companies can highlight emerging best practices and demonstrate market-driven or ethical leadership. Second, in economies with a mandate, examining how leading companies implement these requirements provides concrete benchmarks and practical models. These cases can inform the development of more effective guidelines and showcase successful strategies for communicating complex information to younger audiences.

II. Status of APEC economies

1. Australia

Major platforms like Meta are proactively implementing compliance practices, such as deactivating accounts of users under 16 and sending clear notifications to users to comply with looming social media age restrictions.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

No information was found in relation to this issue.

4. Chile

No information was found in relation to this issue.

5. People's Republic of China

No information was found in relation to this issue.

6. Hong Kong, China

For example, PlayStation has privacy notices designed for young players in Hong Kong, China available in both English and Chinese.

7. Indonesia

No information was found in relation to this issue.

8. Japan

No information was found in relation to this issue.

9. Republic of Korea

There are companies that provide child-friendly privacy policies using terms and illustrations that are easily understandable for children and adolescents. Major companies such as Naver and Kakao also disclose "easy-to-understand privacy policies" for children and adolescents, utilizing pictures, videos, and other materials to fulfill the above obligations.

10. Malaysia

No information was found in relation to this issue.

11. Mexico

No information was found in relation to this issue.

12. New Zealand

No information was found in relation to this issue.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

No information was found in relation to this issue.

15. The Republic of the Philippines

No information was found in relation to this issue.

16. The Russian Federation

No information was found in relation to this issue.

17. Singapore

Organizations whose online products or services are likely to be accessed by children are required to comply with the PDPC's Advisory Guidelines on the PDPA for children's personal data in the digital environment. To be clear, the scope is not limited to products and services that are designed for and aimed specifically at children but also covers products and services that are in fact accessed by children.

18. Chinese Taipei

No information was found in relation to this issue.

19. Thailand

No information was found in relation to this issue.

20. United States

Many companies and platforms adopt “privacy dashboards,” icons, explainers, or age-targeted disclosures (e.g., YouTube Kids, Facebook’s teen privacy center). Industry certifications (e.g., COPPA Safe Harbor) encourage clear, age-appropriate disclosures. The Global CBPR Forum recently adopted new Global CBPR System Program Requirements to increase accountability for processing children’s data. Through the United States’ participation in the Global CBPR Forum, United States companies can certify to the Global CBPR System, a voluntary, multilateral data privacy certification for companies to demonstrate compliance with government-recognized requirements

21. Viet Nam

Companies are obligated to provide notifications; however, there are no specific guidelines on the format or use of child-friendly language tailored for children.

III. Comparative Analysis and Implications

The following table indicates there are examples of Corporate Best Practices were given in each jurisdiction.

Table 18 Corporate Practices and Cases

APEC Economy	Are there examples of Corporate Best Practices? (O/X)
Australia	O
Brunei Darussalam	-
Canada	-
Chile	-
People’s Republic of China	-
Hong Kong, China	O
Indonesia	-
Japan	-
Republic of Korea	O
Malaysia	-
Mexico	-
New Zealand	-
Papua New Guinea	-
Peru	-
The Republic of the Philippines	-
The Russian Federation	-
Singapore	O (Required for relevant services)
Chinese Taipei	-
Thailand	-
United States	O
Viet Nam	-

While legal mandates establish the essential foundation, actual corporate practices reveal how child-friendly transparency is applied in the real world. In several APEC economies, leading companies are already implementing innovative methods to communicate privacy information to younger users, driven either by the need to comply with legal requirements or as a commitment to voluntary best practices. In Korea, for instance, major tech companies such as Naver and Kakao utilize pictures and videos to create "easy-to-understand privacy policies." Similarly, many platforms in the United States employ intuitive privacy dashboards, icons, and dedicated privacy centers for minors, while in Hong Kong, China, PlayStation provides notices specifically tailored for young players.

Beyond the specific regulatory frameworks of individual APEC economies, significant and proactive steps taken by major global operators further illustrate a growing industry trend toward enhanced protection for minors. TikTok, for example, has mandated opt-in consent for personalized advertising for users under 18 and introduced a "bedtime" feature for push notifications to prevent younger teens from receiving alerts late at night. YouTube has also taken substantial measures by removing overly commercial content from YouTube Kids, offering tiered content settings based on age, and enabling break reminders and disabling autoplay by default for users aged 13 to 17. Furthermore, Instagram has integrated age verification into its account creation process and utilizes machine learning to confirm user ages. These efforts are increasingly supported by technology, as platforms deploy AI-based automation for age verification, the identification of inappropriate content, and the enforcement of community standards.

The existence of these case studies provides tangible benchmarks for other companies, demonstrating that it is feasible to translate complex legal requirements into user-friendly interfaces that empower both children and their parents. These examples serve as models for developing effective guidelines and showcase successful strategies that balance compliance with a positive user experience. A prominent example of this is the use of layered notices—where a simple summary links to more comprehensive information—which has emerged as a best practice for satisfying the dual needs of simplicity and disclosure. However, the lack of documented examples in many other economies suggests a potential gap in corporate practice or reporting. For businesses, the lesson is clear: investing in age-appropriate design is becoming a vital competitive differentiator and a key component of a trustworthy brand. Consequently, regulators and industry bodies should continue encouraging work to promote wider adoption of measures that help raise the standard of child data protection across all APEC economies.

Chapter 7 Children or Adolescents' "Rights[26]"

As children and adolescents, so-called digital natives, become increasingly active in online spaces from an early age, the protection of their personal data has gained growing significance. The widespread use of digital devices such as smartphones and computers leads to the accumulation of online information that may later have unexpected and potentially harmful consequences in their adult lives. In this context, data protection rights, including access, rectification, erasure (the "right to be forgotten"), and restriction of processing, play a vital role in enabling minors to protect themselves from future disadvantage.

Among these, the "right to be forgotten," which applies in certain jurisdictions, holds particular importance, as it empowers individuals to request the deletion of past data and prevent its continued circulation. This right can be especially meaningful for young people, whose actions or expressions in their formative years may not reflect their current identity or values.

This section explores the extent to which economies recognize and guarantee data protection rights for minors, whether these rights differ from those of adults, and whether specific measures or initiatives are in place to support children and adolescents in exercising such rights in practice.

Section 1. Children or Adolescents' "Rights" as data subjects

I. Introduction

As data protection laws increasingly recognize the rights of individuals over their personal data, questions arise as to how these rights apply to minors. In particular, there is growing attention on whether children and adolescents are entitled to exercise core data subject rights, such as the right of access, the right to rectification, and the right to restriction of processing, independently, and if so, from what age and under what conditions.

This section examines whether legal frameworks explicitly recognize these rights for minors and whether the exercise of such rights is contingent on the individual's age, maturity, or legal capacity. It also explores whether and to what extent parents or legal guardians are entitled to exercise these rights on behalf of the child or adolescent, either concurrently or exclusively, particularly in cases where the minor lacks legal capacity.

II. Status of APEC economies

1. Australia

[26] In some economies, the following may not be recognized as rights; however, for convenience and in light of recent trends, they will hereinafter be referred to as "rights."

In Australia, the Privacy Act and the Australian Privacy Principles (APPs) apply to individuals of all ages. Specifically, APPs 12 and 13 provide all individuals with the rights to access and correct their personal data, and these rights are not restricted by age. This means that children and adolescents are, in principle, entitled to exercise these rights independently, subject to their capacity to understand and act upon them. The recognition of rights is generally assessed on a case-by-case basis, depending on the minor's maturity and ability to comprehend the nature of the request.

Additionally, the Children's Online Privacy Code, which is currently under development, is expected to offer more detailed guidance on how existing privacy obligations—including those under APPs 12 and 13—should be applied to children. Once finalized, this Code may clarify implementation measures that take into account the specific needs and vulnerabilities of minors in the digital environment.

With regard to parents or guardians, there is currently no explicit legal provision granting them personal data rights over their child's or adolescent's data. Parental rights are not separately recognized under the Privacy Act unless the child is assessed to lack the maturity to make their own decisions, in which case organizations may choose to deal with the parent or guardian as a matter of practical judgment rather than legal entitlement.

2. Brunei Darussalam

Under Brunei Darussalam's Personal Data Protection Order (PDPO), children and adolescents are granted the same personal data rights as adults. These include the right of access (§21), the right to rectification (§22), the right to erasure (§25), and the right to restriction of processing (§25). The law does not distinguish between adults and minors in terms of the scope of these rights, implying that minors may exercise them equally, subject to practical considerations such as capacity.

However, it remains unclear whether parents or legal guardians are granted any specific or derivative rights to act on behalf of their children under the PDPO. No explicit provisions confirming such parental rights were identified in the available materials.

3. Canada

Under Canada's federal privacy law, the Personal Data Protection and Electronic Documents Act (PIPEDA), children and adolescents are entitled to exercise key data subject rights, including the right to access their personal data held by an organization and the right to request corrections to inaccurate or incomplete data. While PIPEDA does not include a formal "right to restriction of processing" akin to the GDPR, individuals generally retain the ability to revoke or withdraw consent for certain uses of their personal data, except where processing is legally required.

According to guidance from the Office of the Privacy Commissioner (OPC), parents or guardians may exercise these rights on behalf of a child or adolescent only in cases where the minor lacks sufficient legal capacity or maturity to do so independently. This determination is made based on the individual circumstances, rather than a fixed age threshold, and reflects a case-by-case approach to assessing a minor's ability to exercise control over their personal data.

4. Chile

Under Chile’s current data protection framework, the Personal Data Protection Law (LPVP), individuals are granted core data subject rights including the right of access, rectification, suppression, and opposition, collectively referred to as ARCO rights. Under the new Personal Data Protection Law (LPPD), these rights will be expanded to include the right to data portability and the right to block data processing. These rights are recognized equally for children and adolescents, meaning minors are in principle entitled to exercise the same rights as adults concerning their personal data.

As of now, there is no explicit provision or confirmed guidance regarding whether parents or legal guardians may exercise these rights on behalf of children or adolescents. The legal framework does not clearly define the scope of parental rights in this context. However, it is worthwhile to note that one of the key promoters emphasized that parents or legal guardians may exercise these rights on behalf of children or adolescents, and that the consent from minors will be considered invalid.

5. People’s Republic of China

In China, both children and their parents or legal guardians are recognized as holding rights in relation to the processing of children's personal data under several legal and regulatory frameworks.

Article 45 of the Personal Information Protection Law (PIPL) grants individuals the right to access their personal data. When an access or copy request is made, the data controller is required to respond without delay. In addition, Article 72 of the Law on the Protection of Minors stipulates that if a parent or guardian requests the correction or deletion of a minor’s personal data, the data controller must promptly comply unless otherwise provided by law or administrative regulations.

Further, Article 10 of the Regulation on the Online Protection of Children’s Personal data requires that, when obtaining consent from a parent or guardian to collect, use, transfer, or disclose a child’s personal data, the data controller must clearly inform them of the procedures for requesting correction or deletion of such data.

These provisions collectively establish a framework in which guardians can exercise data rights on behalf of minors, while also ensuring that both minors and their representatives are informed and empowered in managing personal data.

6. Hong Kong, China

Under Hong Kong, China’s Personal Data (Privacy) Ordinance (PDPO), all individuals—including children and adolescents—are entitled to core data subject rights. Section 18 and Data Protection Principle (DPP) 6 in Schedule 1 of the PDPO provide that data subjects have the right to request access to and correction of their personal data. If a request is refused, the data controller must provide reasons for the refusal. The PDPO does not impose any age-based limitations, and its provisions apply equally to minors.

In addition, Section 18(1) of the PDPO allows a “relevant person” to make a data access request on behalf of a data subject. In the case of a minor, a relevant person is defined as someone with parental responsibility. This means that parents or legal guardians may lawfully exercise data access rights on behalf of their children, particularly when the child is too young to exercise those rights independently.

This framework ensures that both minors and their guardians can engage with personal data rights under the PDPO, while maintaining appropriate protections for those lacking full legal capacity.

7. Indonesia

Indonesia’s Personal Data Protection Law (PDPL, Law No. 27 of 2022) classifies children's personal data as a form of “specific personal data,” thereby subjecting it to heightened protection. Under the PDPL, all data subjects, including children, are granted a range of rights regarding the processing of their personal data. These include the right to access (Article 7), rectify (Article 6), and restrict the processing of their personal data (Article 8), as well as the right to withdraw consent (Article 9) and to limit processing (Article 11).

While these rights are granted directly to the data subject, including minors, no specific provision has been identified that expressly recognizes or regulates the rights of parents or legal guardians to act on behalf of children. The legal framework does not yet clarify whether or how parental authority intersects with a child’s data protection rights under the PDPL. However, given that the PDPL requires parental consent for data processing and minors generally lack full legal capacity under Indonesian Civil Law, the right of parents or legal guardians to exercise these rights on the child's behalf is implied.

8. Japan

Japan’s Act on the Protection of Personal data (APPI) does not contain any provisions that are specifically tailored to minors. As such, children and adolescents are in principle afforded the same personal data rights as adults, including the right to access, correct, or suspend the use of their personal data. These rights apply regardless of age, meaning that minors are recognized as data subjects under the APPI to the same extent as adults.

However, in practice, the exercise of these rights is subject to the individual's legal capacity. Where a minor is not legally competent to provide valid consent or make autonomous decisions about their personal data, a parent or legal guardian may act on their behalf. This is grounded in Article 37, Paragraph 3 of the APPI, which permits data subjects to exercise rights such as access, correction, or suspension of use through a legally authorized agent. Article 13, Paragraph 1 of the Cabinet Order to Enforce the APPI further clarifies that a statutory agent of a minor—such as a parent—may submit such requests.

This framework ensures that minors who lack sufficient decision-making capacity are not excluded from data protection rights; rather, those rights are exercised via their legal representatives. Conversely, if a minor is deemed to possess adequate maturity and understanding, it is generally accepted that they may exercise such rights independently.

9. Republic of Korea

Under Korea’s PIPA, children and adolescents are recognized as data subjects with the same core rights as adults. Articles 35 through 37-2 of the PIPA grant data subjects the right to access their personal data (Article 35), the right to request correction or deletion (Article 36), the right to request suspension of processing or withdrawal of consent (Article 37), and the right to object to fully automated decision-making, including AI-based decisions, and to request an explanation (Article 37-2). These provisions apply equally to minors, ensuring that they are not excluded from the fundamental rights available to all data subjects.

In addition to these rights for minors themselves, the law also provides clear mechanisms for legal guardians to act on behalf of children under the age of 14. Specifically, Article 38(2) of the PIPA permits a legal guardian to request access, correction, or deletion of the child's personal data. This reflects a legal presumption that children under 14 may lack sufficient legal capacity to fully exercise their data rights independently.

Similar provisions exist in other sector-specific laws. Under Article 39-3(2) of the Credit Information Use and Protection Act, the legal guardian of a child under 14 has the right to request access to, correction, or deletion of the child's credit-related personal data. Furthermore, the Act on the Protection and Use of Location Information grants guardians the authority to withhold or withdraw consent for the processing of location data of children under 14 (Article 25(2)). For children under the age of 8, Article 26(4) additionally permits other caregiving protectors, not just legal guardians, to exercise these rights.

Collectively, these provisions demonstrate a robust framework for protecting the personal data of children and adolescents in Korea, balancing the autonomy of minors with the protective role of parents and guardians, particularly in cases where the child is too young to act independently.

10. Malaysia

Under Malaysia's Personal Data Protection Act 2010 (Act 709), children and adolescents are recognized as data subjects and are entitled to core personal data rights, including the right to access and correct their personal data. However, due to the assumption that minors may not fully comprehend the consequences of data processing, these rights are generally exercised on their behalf by a "relevant person." This term refers to a parent, legal guardian, or individual with parental responsibility.

The "relevant person" is authorized to make decisions and submit requests for access or correction in order to ensure that the child or adolescent's data is handled in accordance with the law. This arrangement is intended to safeguard the interests of minors by ensuring that their rights are respected and that their personal data is not misused or mishandled. Thus, while the law formally grants rights to children and adolescents, in practice, those rights are typically exercised through adult representatives to ensure lawful and appropriate data processing.

11. Mexico

In Mexico, children and adolescents are recognized as full data subjects under the Constitution and data protection laws. Article 16 of the Mexican Constitution guarantees all individuals, including minors, the rights to Access, Rectification, Cancellation, and Opposition to the processing of their personal data, commonly known as ARCO rights.

However, because minors are generally considered to lack full legal capacity to exercise these rights independently, their data rights are exercised through legal representation. In accordance with Mexican civil law, parents or legal guardians act on behalf of the child or adolescent to ensure their rights are protected and exercised in their best interests. This delegation of authority is procedural in nature, it does not imply that parents or guardians hold independent data subject rights over the child's personal data.

Thus, while the rights themselves belong to the child or adolescent, legal guardians serve as the channel through which these rights are enforced, especially in contexts such as data

access, correction, or objection to processing. This model ensures that minors' rights are protected while maintaining safeguards appropriate to their legal capacity.

12. New Zealand

Under New Zealand’s Privacy Act, children and young people are granted the same fundamental privacy rights as adults. This includes the right to access and correct their personal data held by agencies, as stipulated in Information Privacy Principles (IPPs) 6 and 7. There are no specific age-based distinctions in the application of these rights; rather, their exercise depends on the individual's maturity and understanding.

Agencies must also adhere to the conditions outlined in IPPs 10 and 11, which limit the use and disclosure of personal data unless certain exceptions apply. These provisions are equally applicable to the personal data of minors, reinforcing the principle that children’s information is afforded the same protections as that of adults under the law.

With regard to the exercise of these rights, the Privacy Act acknowledges that children or adolescents may, in some cases, lack the maturity or cognitive ability to give valid consent or make decisions regarding their personal data. In such cases, a representative may act on their behalf. Importantly, the concept of a representative is not restricted to a parent or legal guardian. Rather, it refers to any individual authorized to exercise the child’s privacy rights, provided they are acting in the best interests of the child.

If it is determined that a parent or guardian is not acting in the child’s best interests, they may not be accepted as the child's representative for privacy-related matters. This approach reflects a nuanced and welfare-based framework, prioritizing the child’s rights and autonomy while providing flexibility in representation.

13. Papua New Guinea

Papua New Guinea’s draft National Data Governance and Data Protection Policy 2024 by the Department of Information & Communications Technology includes provisions for data subject rights such as access, correction, and restriction of processing, and these are expected to apply uniformly to all individuals, regardless of age.

There is currently no indication in the draft policy of separate or enhanced rights for children or adolescents, nor are there any specific provisions outlining the rights of parents or guardians to exercise data rights on behalf of minors. As such, both the scope and application of data subject rights for children remain unclear and under development at this stage.

14. Peru

Under Peru’s Personal Data Protection Law (PDPL), individuals are granted comprehensive data subject rights, including the rights to access, rectify, and restrict the processing of their personal data. These rights apply uniformly to both adults and minors, without differentiation based on age.

However, in the case of minors, the Manual on Personal Data Protection clarifies that these rights, such as the right to access, correct, delete, and restrict processing, are to be exercised by the child’s legal representative. This ensures that minors’ personal data is

protected while acknowledging their limited legal capacity to exercise such rights independently.

15. The Republic of the Philippines

Under the Philippines' Data Privacy Act (DPA), children are recognized as data subjects and are granted the same personal data rights as adults. These include the right to be informed, the right to object, the right to access, the right to correct, the right to rectification, erasure, or blocking, and the right to damages, as outlined in Section 16 of the DPA.

However, due to their lack of legal capacity, children cannot exercise these rights independently. Instead, their rights are exercised on their behalf by their parents or legal guardians, who serve as representatives. It is important to note that these representatives do not possess independent rights to access or control the child's data; they act solely in the child's legal interest. The legal authority of parents or guardians exists only insofar as it supports the exercise of the child's rights under the DPA.

16. The Russian Federation

Under Federal Law No. 152-FZ on Personal Data, all data subjects, including children and adolescents, are granted fundamental rights related to their personal data. These include the right to access, correct, restrict processing, and request deletion of personal data. The law does not distinguish between adults and minors in terms of the scope of these rights.

In practice, however, the exercise of these rights by minors is typically carried out through their legal representatives, such as parents or guardians. The extent of a representative's authority depends on the child's legal capacity and the guardian's legal rights under applicable civil law. This ensures that the data rights of children are protected while aligning with Russia's broader legal framework governing the actions of minors.

17. Singapore

Under Singapore's data protection framework, data protection rights such as access and correction of personal data apply to all individuals, including minors. Parents or legal guardians may exercise these rights on behalf of a minor where the child lacks capacity.

18. Chinese Taipei

Under Chinese Taipei's data protection framework, children and adolescents are granted a full range of data subject rights, including the right to access, correct, suspend processing, delete personal data, and withdraw consent. In practice, where children are too young to provide valid consent, parents or guardians may act on their behalf. While there is no explicit provision detailing the rights of legal representatives, it is understood that parents or guardians may exercise these rights when they are authorized to consent to data processing on behalf of the child.

19. Thailand

Children and adolescents are recognized as data subjects and are granted fundamental rights, including the right to access, rectification, erasure, and restriction of processing. Section 20 of the PDPA confirms that where the consent of a parent or guardian is required for the processing of a minor's data, the parent or guardian is also authorized to exercise the data subject rights on the child's behalf, effectively balancing the child's rights with the parental protective role.

20. United States

The Children's Online Privacy Protection Act (COPPA) grants parents the rights to access and delete the personal data of their children under age 13 and to prevent further collection or use.

As noted previously, within the United States, several states have relevant privacy statutes that complement federal law. For example, under California state law, both the California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA), explicitly recognize data protection rights for minors, including the right to access, correct, and delete personal data, as well as the right to opt out of the sale or sharing of personal data with third parties.

For minors under the age of 13, these rights are exercised by their parents or legal guardians, in accordance with both CCPA/CPRA and federal law. Notably, the law prohibits the sale or sharing of a minor's personal data without affirmative consent: for adolescents aged 13 to 15, such consent must come directly from the minor, while for children under 13, verifiable parental consent is required.

21. Viet Nam

Under Decree No. 13/2023/ND-CP, children and adolescents in Viet Nam are granted the full spectrum of data subject rights, including the rights to be informed, give and withdraw consent, access their data, request erasure, restrict processing, request provision, and object to processing, as set out in Article 9. These rights, however, are exercised through their parents or legal guardians, as minors are not considered legally capable of exercising these rights independently.

Article 20 of the Decree mandates that the processing of children's personal data must be based on parental or guardian consent, reinforcing the principle that all related rights must also be exercised by those legal representatives. This is further supported by the Law on Children (2016), which designates parents and guardians as the child's lawful representatives and entrusts them with the responsibility of protecting the child's personal data and privacy rights.

III. Comparative Analysis and Implication

The following table presents a comparative analysis of the legal frameworks across APEC economies concerning the recognition of children's and adolescents' data subject rights and the role of parents or guardians in exercising these rights.

Table 19 Children or Adolescents' "Rights" as data subjects

Economy	Children/Adolescents Have Data Rights	Parental/Guardian Rights
Australia	Yes (case-by-case based on maturity)	Not explicitly, but possible if child lacks capacity
Brunei Darussalam	Yes	Not explicitly provided
Canada	Yes	Yes, if minor lacks legal capacity
Chile	Yes	Not explicitly provided
People's Republic of China	Yes	Yes, guardians can act on behalf
Hong Kong, China	Yes	Yes, 'relevant person' (e.g., parent) allowed
Indonesia	Yes	Not explicitly provided
Japan	Yes	Yes, legal guardian may act if child lacks capacity
Republic of Korea	Yes	Yes, guardians can act under specific laws
Malaysia	Yes	Yes, 'relevant person' authorized
Mexico	Yes	Yes, exercised via legal guardian
New Zealand	Yes	Yes, if acting in best interest
Papua New Guinea	Yes (draft policy)	Not specified
Peru	Yes	Yes, legal representative exercises rights
The Republic of the Philippines	Yes	Yes, via parents/guardians
The Russian Federation	Yes	Yes, depending on child capacity
Singapore	Yes	Yes, if the child lacks capacity
Chinese Taipei	Yes	Yes, in practice
Thailand	Yes	Yes, legal guardian may act if child lacks capacity
United States	Yes (CCPA/COPPA)	Yes, under 13 via parents
Viet Nam	Yes	Yes, through legal representatives

The analysis across APEC economies confirms a universal commitment to granting data subject rights—such as access, rectification, and restriction—to children and adolescents. The core divergence among jurisdictions lies not in the existence of these rights, but in the mechanisms by which they are exercised and the specific age or maturity thresholds that govern independent action. Within prevailing legal frameworks, the legal incapacity of minors

does not result in a loss of rights; rather, it necessitates a formal delegation of authority to ensure the child's best interests are consistently protected.

To navigate this complexity, a balanced regulatory approach—often referred to as a "sliding scale"—is essential. Under this model, the degree of a child's independent control over their data increases in tandem with their age and maturity. Consequently, APEC economies should be encouraged to establish clear benchmarks to define the age of digital consent and specify which rights, such as access or erasure, transition to the minor at various stages. Building on these benchmarks, regulations should include nuanced mechanisms that allow legal representatives to act on behalf of younger children while carefully avoiding undue infringement on the privacy of older adolescents who demonstrate the capacity to manage their own data independently.

Section 2. The "Right to be Forgotten"[27] for Children and Adolescents

I. Introduction

The "right to be forgotten", allowing individuals to request the deletion of their personal data, has become an increasingly important tool in the digital age, particularly for children and adolescents. As minors often engage in online activity before fully understanding its long-term implications, the ability to erase or suppress past digital traces is essential in protecting them from future harm.

This section investigates whether demanding erasure is generally recognized under domestic data protection laws, and whether any specific provisions exist to address requiring the deletion of personal data in the context of children and adolescents. It also explores whether any government-led or private-sector initiatives have been introduced to facilitate the requested deletion of personal data by minors.

II. Status of APEC economies

1. Australia

Australia does not currently recognize a general "right to erasure" under its privacy framework. While individuals do not have an explicit legal right to request deletion of their personal data, they are entitled under Australian Privacy Principle (APP) 13.1 to request corrections if their personal data is inaccurate, out-of-date, incomplete, irrelevant, or misleading. In practice, such correction may take the form of deletion, where appropriate under the circumstances.

[27] While this is a well-known term, not every economy recognizes this as a legal right.

If an organization refuses to make the requested correction, it must provide written reasons for the refusal along with information on how the individual may lodge a complaint. This applies to all individuals regardless of age, including children and adolescents, although capacity and maturity may affect how such requests are managed in practice.

The broader question of whether to introduce a formal right to erasure—particularly in line with international developments—was addressed in the Australian Government's comprehensive Privacy Act Review, published in February 2023. Although the first tranche of reforms, implemented through the Privacy and Other Legislation Amendment Act 2024 (Cth), did not include enhanced individual rights, further legislative reform is under consideration. This may open the door for the future introduction of an explicit erasure right, potentially including child-specific provisions, but no such right exists at present.

2. Brunei Darussalam

Brunei Darussalam's Personal Data Protection Order (PDPO) recognizes a general right to erasure under Section 25. This right is available to all individuals, including children and adolescents, without any age-based distinction. However, the PDPO does not contain any specific provisions establishing a separate or enhanced "right to be forgotten" tailored to minors. The law treats all data subjects equally in this regard.

3. Canada

Canada does not formally guarantee a general or explicit "right to be forgotten" under PIPEDA. However, individuals, including children and adolescents, may request the deletion of their personal data from organizations. In addition, PIPEDA provides individuals with the right to withdraw consent for the processing of their data, which may result in deletion where continued processing is not required by law.

The Office of the Privacy Commissioner (OPC) encourages organizations to accommodate requests for the removal or deletion of children's online accounts and data, whether initiated by the child (if mature enough) or by a parent. While not legally mandated, this practice reflects a flexible, rights-respecting approach to protecting minors in digital environments.

Furthermore, in its exploratory consultation for a Children's Privacy Code, the OPC recommended that organizations support deletion or de-indexing mechanisms that allow young individuals to correct mistakes or retract information they previously shared but no longer wish to remain online. Although these recommendations are not yet binding, they signal a growing recognition of the importance of providing children with greater control over their digital footprint.

4. Chile

Chile does not explicitly recognize a statutory "right to be forgotten" under its current data protection laws. However, individuals, including children and adolescents, may seek the deletion of their personal data through a constitutional remedy known as recurso de protección, which is provided under Article 20 of the Chilean Constitution. This judicial mechanism allows individuals to request the protection of their fundamental rights, including the right to privacy, and has been used in practice to demand the erasure of personal data from online platforms.

There are no specific legal provisions or institutional programs that establish a separate right to be forgotten for minors, nor have any dedicated public or private initiatives been identified that facilitate the exercise of such a right for children and adolescents. In practice, the recurso de protección remains the primary avenue through which minors may attempt to remove personal data, subject to judicial discretion.

5. People's Republic of China

General right to deletion (erasure) for all individuals are recognized. More specifically for minors, the law grants parents or guardians the right to request the correction or deletion of a minor's personal data if it has been collected or processed in violation of laws or agreements. While the law does not use the specific term "right to be forgotten," it establishes a legal mechanism for erasure, which applies to children's data.

6. Hong Kong, China

Hong Kong, China's Personal Data (Privacy) Ordinance (PDPO) does not explicitly recognize a "right to be forgotten" in the form commonly found under laws such as the EU GDPR. However, the PDPO does impose certain erasure-related obligations on data users. Specifically, Data Protection Principle (DPP) 2(2) and Section 26 of the PDPO require data users to erase personal data once the purpose for which the data was collected is no longer being served and retention is no longer necessary.

Thus, although individuals in Hong Kong, China, including children and adolescents, do not possess a formal right to request deletion of their data on demand, the PDPO establishes a statutory duty for data users to delete outdated or unnecessary personal data.

7. Indonesia

Indonesia's Personal Data Protection Law (PDPL) expressly grants data subjects the right to request the deletion or destruction of their personal data, as set out in Article 8. This right applies generally to all individuals, including children and adolescents, and is not limited by age. However, the law does not contain a specific provision establishing a separate or enhanced "right to be forgotten" exclusively for minors.

As of the time of review, no dedicated domestic or private-sector initiatives have been identified that focus on implementing or facilitating the right to be forgotten for children and adolescents, such as systems for deleting online content created during childhood or preventing such content from appearing in search results.

8. Japan

Japan's Act on the Protection of Personal data (APPI) does not explicitly define or guarantee a "right to be forgotten" in the same sense as under the EU General Data Protection Regulation (GDPR). The term "right to be forgotten" is not used in the APPI, and since the concept may carry various interpretations in different jurisdictions, ranging from erasure of personal data to de-indexing from search engines, the Japanese law does not provide a clear legal basis for it as a unified right.

Nevertheless, the APPI does contain provisions that allow individuals, including minors, to request the suspension or deletion of their retained personal data under certain conditions. Article 35, Paragraph 1 of the APPI enables a data subject to request that a business ceases to use or deletes their personal data when that data has been processed in violation of Articles 18, 19, or 20, such as when obtained improperly or used beyond the original stated purpose. This form of remedy applies specifically to “retained personal data,” as defined in Article 16, Paragraph 4, which refers to personal data that the business has the authority to manage (i.e., disclose, correct, erase, or stop using), with some exceptions for data that could harm public interests if disclosed.

9. Republic of Korea

Under Article 36 of Korea’s PIPA, data subjects have the right to request the deletion of their own personal data. However, this right is limited in scope and does not extend to the deletion of content created or posted by third parties. Consequently, a broad "right to be forgotten", which typically includes de-indexing or removing third-party content from search results—is not explicitly recognized under Korean law. Additionally, the PIPA does not contain a specific provision granting an enhanced or separate right to erasure for children and adolescents.

Recognizing that children and adolescents may be less experienced or empowered in exercising their data rights, Korea’s Personal data Protection Commission launched a specialized initiative in April 2023 known as the “Eraser Service.” This program is designed to assist minors in requesting the deletion of content they created themselves during their childhood or teenage years, particularly social media posts or online entries that contain personal data. The service aims to help individuals mitigate long-term reputational risks or harm stemming from content shared when they were not fully aware of the consequences of public digital expression.

While not a legal right per se, the Eraser Service represents a significant policy initiative that facilitates the practical exercise of erasure rights by children and adolescents, reflecting an effort to strengthen youth data protection through supportive mechanisms beyond formal statutory provisions.

10. Malaysia

Malaysia’s Personal Data Protection Act 2010 (Act 709) does not explicitly recognize a general “right to erasure” or “right to be forgotten.” There is no statutory provision that allows individuals, whether adults or minors, to formally request the deletion of their personal data as a matter of right. However, Act 709 incorporates the Retention Principle, which requires that personal data must not be retained longer than is necessary to fulfill the purpose for which it was collected. Once the data is no longer needed, it must be erased. This principle applies equally to the personal data of children and adolescents, but it does not amount to an active or discretionary right for the data subject to initiate erasure.

There are currently no government or private-sector initiatives in Malaysia that specifically support the exercise of a right to be forgotten for minors. Nonetheless, some protection is afforded to children in the digital space under the Communications and Multimedia Act 1998 (CMA). The Malaysian Communications and Multimedia Commission (MCMC), operating under the Ministry of Communication, is responsible for regulating online content and may take enforcement action against websites that host harmful or inappropriate material. While the CMA does not provide for data subject rights per se, it empowers MCMC to intervene in

cases where online content may negatively affect minors, contributing to a safer digital environment.

11. Mexico

Mexican data protection laws recognize a general right to erasure, formally referred to as the “right to cancellation”. This right is available to all data subjects, including children and adolescents, but is not specifically labeled or structured as a distinct “right to be forgotten” in the legal framework. Moreover, no special version of this right exists exclusively for minors.

In the private sector, the right to cancellation is codified in Article 24 of the Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP). It allows individuals to request that their personal data be removed from the systems and databases of data controllers. A similar provision exists for the public sector under Article 40 of the General Law on Protection of Personal Data Held by Obligated Subjects (LGPDPPSO), which enables individuals to request the erasure of their personal data from official files, registries, and systems managed by public authorities.

While these provisions provide a general legal foundation for data erasure, there is currently no enacted legislation in Mexico that establishes a dedicated right to be forgotten, whether for adults or for minors. However, several legislative initiatives have been introduced, both at the federal and local levels, aiming to formalize such a right, particularly in response to growing concerns about digital reputation and privacy. As of now, none of these initiatives have been approved by Congress.

12. New Zealand

New Zealand’s privacy law does not formally recognize a “right to erasure” or “right to be forgotten.” However, under the Privacy Act, individuals, including children and adolescents, have the right to request correction of their personal data. In practice, this can include deletion of information, depending on the context and the agency’s obligations.

There is no distinct legal framework or provision granting a separate or enhanced right to be forgotten for minors. Furthermore, as of now, no government or private initiatives exist in New Zealand that support child-specific erasure rights, such as programs assisting minors in deleting online content created during childhood.

13. Papua New Guinea

The draft National Data Governance and Data Protection Policy 2024, prepared by Papua New Guinea’s Department of Information & Communications Technology, includes provisions for a right to erasure. However, this right is formulated as a general data subject right and is not differentiated by age. There is no specific clause establishing a separate or enhanced right to be forgotten for children or adolescents.

Additionally, there are no known government or private initiatives in Papua New Guinea that support child-specific erasure services, such as programs assisting minors in deleting personal data posted during childhood or adolescence.

14. Peru

Peru's Personal Data Protection Law (PDPL) recognizes the right to deletion, also referred to as the right to be forgotten, as part of the fundamental rights granted to data subjects. This right is available to all individuals, including children and adolescents. However, the law does not provide a separate or specially tailored formulation of the right to be forgotten that applies exclusively to minors.

In terms of enforcement, the Peruvian Data Protection Authority has taken notable steps to uphold the right to be forgotten. In 2016, it issued a landmark decision legally affirming this right and imposed a fine of USD 75,000 on Google for its failure to comply with a deletion request. However, this case did not involve children or adolescents, and there are currently no known public or private initiatives specifically designed to support minors in exercising this right, such as services for deleting personal content posted during childhood or blocking it from search engine results.

15. The Republic of the Philippines

The Philippines recognizes a general right to erasure, also referred to as the right to be forgotten, under its Data Privacy Act. This right is available to all data subjects, including children and adolescents. However, the law does not provide a specific or enhanced version of this right that applies exclusively to minors.

Furthermore, there are no known government or private-sector initiatives in the Philippines that support minors in exercising the right to be forgotten.

16. The Russian Federation

Russia's Federal Law No. 152-FZ on Personal Data does not explicitly define or refer to a "right to be forgotten." However, individuals, including children and adolescents, may request the deletion of their personal data or demand that such data no longer be made publicly available. These mechanisms provide substantive protection comparable to the right to be forgotten, even if not framed under that specific terminology.

Despite this general protection, there is no distinct legal provision establishing a separate or enhanced erasure right specifically for minors. Likewise, there are no government programs or private-sector initiatives currently in place that specifically support children or adolescents in exercising erasure rights.

17. Singapore

Singapore's Personal Data Protection Act (PDPA) does not provide for a right to erasure, and the concept of the "right to be forgotten" is not expressly recognized under current law. However, organizations have a retention obligation requiring them to cease retaining personal data or to anonymize it once it is no longer needed. Individuals are also allowed to withdraw consent to the use of their personal data, which when read with the retention obligation would require an organization to delete this data accordingly. In substance, these have a similar legal effect as a right to be forgotten. Such rights are also applicable when children are data subjects.

18. Chinese Taipei

Chinese Taipei guarantees the right to erasure of personal data to all individuals, including both adults and minors. This right is generally recognized under its data protection laws without distinguishing between age groups, meaning that children and adolescents are equally entitled to request the deletion of their personal data.

However, there is no specific legal provision establishing a separate or enhanced version of the right to be forgotten for minors. In addition, there are no known government or private-sector initiatives in Chinese Taipei that focus on supporting children or adolescents in exercising this right.

19. Thailand

PDPA explicitly provides a right to erasure under Section 33. This section allows data subjects to request the data controller to erase, destroy, or de-identify personal data under specific circumstances, such as when the data is no longer necessary or when consent is withdrawn. This right applies generally to all data subjects, including children and adolescents, but there is no specific, enhanced version of this right tailored exclusively for minors.

20. United States

In the United States, COPPA safeguards parents' right to direct that an operator covered by COPPA delete a child's personal information. In addition, several state-level privacy laws recognize a right to delete personal data for children and adolescents, even though the term "right to be forgotten" is not formally used. Under the California Consumer Privacy Act (CCPA), individuals under the age of 18 may request deletion of personal data collected by a business. This protection is subject to certain exceptions, such as where the business is legally required to retain the information for compliance or public interest reasons.

Beyond California, other states—including Colorado, Connecticut, and Utah—have adopted similar privacy laws that grant deletion protection to individuals under 18, reflecting a growing trend in United States state legislation to provide minors with greater control over their digital footprint.

California has also implemented a dedicated statute known as the California Eraser Law, which specifically empowers users under the age of 18 to request the removal of content or information they have posted on social media platforms. This law complements broader CCPA rights and offers practical protections tailored to the behaviors of minors in digital environments.

In terms of private-sector efforts, companies like The Walt Disney Company have operationalized these obligations by allowing minors—particularly those under 18 residing in California—to submit content deletion requests via dedicated privacy contact channels. These efforts represent a practical extension of erasure rights for youth users.

21. Viet Nam

Viet Nam's Decree No. 13/2023/ND-CP explicitly guarantees the right to data erasure for all data subjects under Article 9(1)(e). This right applies equally to children and adolescents but is not framed as a separate or enhanced "right to be forgotten" for minors. There are currently no distinct provisions that specifically address children in this context.

As of now, there are no known government or private-sector initiatives dedicated to supporting minors in exercising erasure rights, such as programs for deleting personal content created during childhood. However, with the recent adoption of Decree No. 13 and increasing public awareness around data protection, there is potential for future development of child-specific guidance or services, especially concerning content shared by minors on social media and other online platforms.

III. Comparative Analysis and Implication

The following table presents a comparative analysis of the legal frameworks and practical initiatives across APEC economies concerning the Right to be Forgotten for children and adolescents.

Table 20 The "Right to be Forgotten" for Children and Adolescents

Economy	General Right to Erasure	Applies to Children/Adolescents	Child-Specific Right	Public/Private Initiatives
Australia	No general right to erasure; correction possible (APP 13.1)	No	No child-specific right	Under review; no initiatives yet
Brunei Darussalam	Yes (Section 25 PDPO)	Yes	No	None identified
Canada	No explicit right; deletion via consent withdrawal	Yes	No	OPC recommends deletion for children; not binding
Chile	No explicit law; deletion via constitutional remedy	Yes	No	No initiatives identified
People's Republic of China	Yes (PIPL Art. 47)	Yes	No	None identified
Hong Kong, China	No formal right; deletion required when no longer needed	Yes	No	None identified
Indonesia	Yes (PDPL Art. 8)	Yes	No	None identified
Japan	No explicit right; limited deletion possible under APPI	Yes	No	None identified

Republic of Korea	Yes (PIPA Art. 36)	Yes	No	PIPC Eraser Service (since 2023)
Malaysia	No explicit right; retention principle applies	Yes	No	MCMC regulates harmful content
Mexico	Yes (cancellation right)	Yes	No	Legislative efforts pending
New Zealand	No formal right; deletion possible under correction	Yes	No	None identified
Papua New Guinea	Yes (draft policy)	Yes	No	None identified
Peru	Yes (PDPL)	Yes	No	No child-specific programs
The Republic of the Philippines	Yes (Data Privacy Act)	Yes	No	None identified
The Russian Federation	Yes	Yes	No	None identified
Singapore	No	No	No	None identified
Chinese Taipei	Yes	Yes	No	None identified
Thailand	Yes (PDPA Sec.33)	Yes	No data	No data
United States	Yes (state laws)	Yes	Yes (e.g., CA Eraser Law)	Yes (e.g., Disney content deletion)
Viet Nam	Yes (Decree 13/2023)	Yes	No	Potential in future, no current initiatives

The analysis of the Right to be Forgotten across APEC economies reveals a growing convergence toward empowering individuals to control their digital footprint, yet significant variances remain in how this right is structured for minors. While the majority of jurisdictions—including China; Indonesia; the Philippines; and Thailand—now grant a general statutory right to erasure that applies equally to children, only a few have implemented targeted mechanisms to address the unique vulnerabilities of youth. The United States stands out with California's "Eraser Law," which provides a specific statutory right for minors to delete self-posted content, directly addressing the risks of impulsive online behavior. Similarly, Korea has introduced the "Eraser Service," a government-led initiative that supports minors in exercising their deletion rights practically, even in the absence of a separate child-specific law. In contrast, economies like Australia; Hong Kong, China; and Singapore rely on indirect mechanisms such as correction rights or retention limitations rather than a direct "right to be forgotten."

This landscape suggests that while the fundamental authority to delete data is becoming a global standard, the development of specialized "second chances" for digital natives remains an emerging frontier, led by select economies adopting proactive, child-centric interventions. To bridge these existing gaps, APEC economies should encourage regulatory approaches that strengthen protection regarding deletion of personal data originating from children or adolescents, particularly for content they posted themselves during their minority. Furthermore, consideration should be given to extending these protections beyond merely delisting search results to requiring that data controllers actively erase data from all processing systems, thereby ensuring a "clean slate" as the individual reaches adulthood. By also implementing mandatory and highly visible data retention policies specific to minors, economies can ensure that the eventual exercise of this right becomes a practical reality rather than a theoretical possibility.

Chapter 8 Prohibition of Certain Processing Purposes or Types of Personal Data Involving Children or Adolescents

Children and adolescents are in critical stages of cognitive, social, and emotional development, making them particularly vulnerable to certain types of personal data processing, especially profiling and other forms of automated decision-making. Such processing may result in undue influence, discriminatory outcomes, or manipulative targeting that disproportionately affects young individuals.

The rapid increase in minors' online engagement, coupled with the advancement of AI technologies, has further intensified these risks. Of particular concern is the unauthorized use of children's images, voices, or likenesses in deepfake content, which can cause severe psychological harm and open the door to potential exploitation or abuse.

Given these heightened vulnerabilities, it is imperative to understand how different jurisdictions regulate and, in some cases, prohibit specific processing purposes or categories of personal data when it involves children or adolescents. This chapter provides an overview of relevant legal frameworks and explores how regulatory authorities around the world seek to protect minors from harmful or inappropriate data processing practices.

Section 1. Profiling and Targeted Advertising Involving Children or Adolescents

I. Introduction

With the rise of digital platforms and AI-driven profiling, children and adolescents are increasingly exposed to targeted advertising based on their online behavior. Given their developmental stage, minors are more vulnerable to manipulation and may not fully understand how their data is used.

In response, many jurisdictions have introduced laws or regulations that prohibit or restrict the processing of children's personal data for purposes such as profiling and behavioral advertising. These measures aim to prevent unfair influence, discrimination, and exploitation.

This section reviews whether and how different economies regulate or prohibit the use of children's personal data for specific purposes, focusing on profiling and targeted advertising.

II. Status of APEC economies

1. Australia

Australia does not currently have specific legal provisions that prohibit profiling of children or adolescents for targeted advertising.

Under APP 7 entities must not use or disclose personal data for the purposes of direct marketing, unless the individual has consented to such use and the individual must be provided with a simple means of opting out of direct marketing that uses their personal data. Additionally, entities may disclose an individual's personal data to a third party for direct marketing by the third party where the information has been obtained from someone other than the individual to whom the information relates and it is impracticable to obtain the individual's consent. The Children's Online Privacy Code (currently being developed), may provide further specification on how existing requirements are to be complied with, with respect to children. This Code may also include additional requirements that aren't inconsistent with existing obligations.

The Criminal Code Amendment (Deepfake Sexual Material) Act 2024 introduced serious criminal penalties on those who share sexually explicit material without consent, however it does not apply to children. One of the elements of the offence requires the person to be, or appear to be, over 18. This is because the offence includes consent requirements, noting it's not appropriate for children to be able to consent.

2. Brunei Darussalam

While the PDPO does not contain a specific statutory prohibition on profiling children for targeted advertising, general data protection principles regarding consent and purpose limitation apply. There is no explicit ban found in the current legislation.

3. Canada

Canada's federal privacy law, the Personal Data Protection and Electronic Documents Act (PIPEDA), does not contain an explicit statutory prohibition on profiling or using children's personal data for targeted advertising purposes. However, the Office of the Privacy Commissioner of Canada (OPC), which enforces PIPEDA, has issued guidance clarifying its position on this matter. According to the OPC, practices such as tracking, profiling, or targeting children for marketing or behavioral advertising purposes generally fail to satisfy the standard of "meaningful consent" required under PIPEDA. This is due to children's limited capacity to fully understand the implications of such data processing activities, which challenges the validity of their consent. Additionally, such practices may not meet the threshold for a legitimate business interest that could override the child's right to privacy.

4. Chile

In Chile, the recently amended Personal Data Protection Law (LPPD) introduces new safeguards concerning automated processing of personal data, including profiling. Specifically, Article 8 of the LPPD establishes the right of data subjects to object to and not be subject to decisions based solely on automated processing. This provision includes the right to object to profiling, which encompasses the use of personal data, such as that of children and adolescents, for targeted advertising or other similar purposes. While the law does not provide a child-specific prohibition, the general right to object to profiling applies to all individuals and serves as a legal basis to restrict such data processing activities involving minors.

5. People's Republic of China

The use of children's personal data for profiling and automated decision-making is strictly regulated under existing laws. The PIPL mandates that automated decision-making must be transparent and fair, and requires strict protection for the sensitive personal information of minors under 14 (Article 28).

Regulation on the Protection of Minors in Cyberspace stipulates that online product and service providers shall not carry out commercial marketing to minors by means of automatic decision-making.

More specifically, the Internet Information Service Algorithmic Recommendation Management Provisions, effective March 2022, explicitly prohibit algorithm recommendation service providers from pushing information to minors that may induce them to internet addiction or is contrary to social morality.

6. Hong Kong, China

In Hong Kong, China, there is no specific or standalone regulation that explicitly prohibits the use of children’s or adolescents’ personal data for particular purposes such as profiling for targeted advertising. However, such practices are subject to the general data protection framework established under the Personal Data (Privacy) Ordinance (PDPO).

Specifically, Data Protection Principle (DPP) 3 in Schedule 1 to the PDPO governs the use of personal data. It provides that personal data must not be used for any purpose other than the purpose for which the data was originally collected or for a directly related purpose, unless the prescribed consent of the data subject has been obtained. This requirement applies irrespective of the data subject’s age.

In the context of profiling for targeted advertising, if this was not part of the original stated purpose at the time of data collection, such use would generally be considered impermissible unless express consent is secured. While the law does not establish special protections for minors in this regard, the same legal standards apply to children and adolescents, meaning that any data processing beyond the original scope, including profiling, would require valid consent.

7. Indonesia

In Indonesia, Government Regulation No. 17 of 2025 (GR 17/2025) strictly prohibits profiling of children and adolescents. This prohibition applies regardless of the purpose, including for targeted advertising or other automated decision-making processes. The regulation reflects a broader commitment to safeguarding minors from potentially harmful data practices by explicitly banning any form of profiling that could exploit their personal data or affect their rights and well-being.

8. Japan

In Japan, the Act on the Protection of Personal data (APPI) does not explicitly prohibit the use of minors’ personal data for specific purposes such as profiling for targeted advertising. However, the use of profiling techniques that direct minors to sexual or violent content is prohibited under separate legislation outside the APPI framework. These restrictions aim to protect children and adolescents from exposure to harmful material, even though there is no specific ban on profiling for commercial purposes under Japan’s main data protection law.

9. Republic of Korea

In Korea, there is no explicit statutory prohibition under the PIPA against profiling children or adolescents for the purpose of targeted advertising. However, if behavioral data of children or adolescents is combined with personally identifiable information (PII) for advertising purposes, service providers must clearly inform users of the data collection and usage details, including the purpose, types of data combined, and retention period, and obtain prior consent. In the case of minors, such consent must be obtained from a legal guardian.

Furthermore, the Personal data Protection Commission (PIPC) has issued guidance documents such as the Guide on the Protection of Children and Adolescents' Personal data and Policy Measures for Protecting Online Behavioral Information Used in Targeted Advertising. These materials recommend that targeted advertising to children be minimized. Even when individuals are not directly identifiable, if the user is known to be a child—or if the service is primarily used by children, data controllers are advised not to process behavioral data for targeted advertising purposes.

10. Malaysia

In Malaysia, the Personal Data Protection Act 2010 (Act 709) does not contain an explicit prohibition on profiling children or adolescents for targeted advertising. However, it imposes restrictions that indirectly regulate such practices. Under the Act’s General Principle, personal data must be collected and processed for a lawful purpose that is directly related to the activities of the data user. This principle limits the processing of personal data for secondary purposes, such as profiling for targeted advertising, unless specific consent is obtained.

When it comes to children and adolescents under the age of 18, consent for data processing must be obtained from a parent, legal guardian, or a person with parental responsibility. This requirement serves as a safeguard to ensure that minors’ personal data is not used for targeted advertising or similar activities without proper authorization. While the law stops short of imposing a blanket ban on profiling, the consent requirement for minors creates a framework through which such data processing is subject to additional scrutiny and protection.

11. Mexico

In Mexico, there are no explicit legal provisions that categorically prohibit the use of children’s or adolescents’ personal data for specific purposes such as profiling for targeted advertising. However, such practices are subject to stringent legal requirements under the economy’s data protection laws, particularly those related to purpose limitation and consent.

In the case of minors, who are legally recognized as a vulnerable group, any processing of sensitive personal data, including profiling, requires express and written consent from the child’s parents or legal guardians. These consent requirements act as a safeguard that effectively limits the use of minors’ data for targeted advertising, even in the absence of an explicit statutory prohibition. Furthermore, the best interests of the child must be prioritized in all data processing activities involving minors, adding another layer of protection against potentially exploitative uses such as behavioral profiling. Thus, while not formally banned,

the use of minors' personal data for targeted advertising in Mexico is significantly constrained in practice by existing legal standards.

12. New Zealand

In New Zealand, there are currently no specific legal provisions that prohibit the use of children's or adolescents' personal data for particular purposes such as profiling for targeted advertising.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

In Peru, while there is no explicit prohibition on the use of children or adolescents' personal data for specific purposes such as profiling for targeted advertising, the Personal Data Protection Law (PDPL) establishes strict requirements concerning transparency in data processing. This principle obliges data controllers to clearly inform data subjects about the purposes for which their data will be used, including whether profiling is involved. Given this obligation of transparency, the processing of children's personal data for purposes such as profiling or behavioral targeting could be problematic if not clearly disclosed and consented to in a meaningful and informed manner.

15. The Republic of the Philippines

In the Philippines, there are currently no specific legal provisions that prohibit the use of children's or adolescents' personal data for particular purposes such as profiling for targeted advertising.

16. The Russian Federation

In Russia, Federal Law No. 152-FZ on Personal Data does not explicitly prohibit the profiling or use of children's personal data for purposes such as targeted advertising. However, such practices may be implicitly restricted under existing legal principles. Specifically, the law imposes strict requirements for processing sensitive personal data, emphasizes the purpose limitation principle, and mandates that data processing must be lawful and proportionate. These general provisions could functionally limit the use of children's personal data for profiling or targeted marketing, particularly where it involves sensitive or excessive data use. Nonetheless, there is no express statutory ban on such practices specifically targeting children.

17. Singapore

While there is no total ban, the PDPC's Advisory Guidelines on the PDPA for Children's Personal Data explicitly state that organizations should avoid profiling children for the purpose of targeting them with marketing messages, as children may not understand the

nature of such processing. It is not a statutory ban but a strong regulatory expectation that failure to obtain valid (parental) consent for such non-obvious purposes would be a breach.

18. Chinese Taipei

In Chinese Taipei, while there is no specific prohibition under the Personal Data Protection Act (PDPA) that targets the processing of children's or adolescents' personal data for specific purposes such as profiling for targeted advertising, the PDPA does impose general restrictions that effectively limit such practices. According to the PDPA, if a data subject opts out of receiving marketing communications, private entities must immediately cease using the individual's personal data for marketing purposes, including personalized advertising or recommendation services. Moreover, when contacting a data subject for marketing purposes for the first time, the entity is required to provide a clear and accessible opt-out mechanism. These safeguards apply regardless of the data subject's age and serve as a de facto limitation on the use of personal data for targeted advertising, including when children or adolescents are involved.

19. Thailand

The PDPA does not explicitly ban profiling. However, Section 30 gives data subjects the right to object to the collection, use, or disclosure of personal data for the purpose of direct marketing. This applies to minors (exercised via guardians). Additionally, processing for marketing without consent is generally prohibited unless it falls under Legitimate Interest, which is hard to justify for minors.

20. United States

In the United States, regulatory frameworks exist at both the federal and state levels to restrict the processing of children and adolescents' personal data for purposes such as profiling and targeted advertising. At the federal level, COPPA requires that certain operators of websites and online services obtain separate verifiable parental consent before disclosing personal data of children under the age of 13 to third parties for purposes such as targeted marketing.

Within the United States, several states have relevant privacy statutes that complement federal law. For example, New York's Child Data Protection Act (CDPA) extends protections to minors up to 18 years of age. Under the CDPA, the processing of personal data of individuals within this age group requires prior consent. For children under 13, compliance with COPPA remains mandatory. However, for users between ages 13-17 the CDPA permits processing of personal data without consent only when it is strictly necessary for the provision or maintenance of a requested service or for specific legal purposes. Importantly, the CDPA guidelines clarify that "internal business operations," including marketing and advertising, do not qualify as "strictly necessary" purposes. Accordingly, such uses would still require express consent, further limiting the use of children's and adolescents' data for profiling or advertising.

21. Viet Nam

Under Viet Nam's Decree No. 13/2023/ND-CP on Personal Data Protection, Article 8 outlines a list of prohibited acts, which includes restrictions relevant to the use of personal data for purposes such as profiling or targeted advertising involving children or adolescents.

III. Comparative Analysis and Implication

The following table presents a comparative analysis of the legal frameworks across APEC economies concerning the prohibition of personal data processing for specific purposes, such as profiling and targeted advertising involving children or adolescents.

Table 21 Profiling and Targeted Advertising Involving Children or Adolescents

Economy	Regulation Summary on Profiling for Targeted Advertising
Australia	No explicit prohibition; APP 7 and Children's Online Privacy Code (in development) regulate use/consent requirements
Brunei Darussalam	No information available
Canada	No explicit prohibition; OPC guidance limits profiling/targeting children due to consent concerns
Chile	Right to object to profiling under Article 8 of LPPD (applies generally)
People's Republic of China	Restriction under PIPL (Art. 24); prohibition on profiling that induces addiction
Hong Kong, China	No explicit child-specific law; PDPO DPP 3 requires original purpose or consent
Indonesia	Explicit prohibition under GR 17/2025
Japan	No explicit prohibition in APPI; other laws prohibit profiling exposing minors to harmful content
Republic of Korea	No explicit ban; requires consent and prior notice; PIPC guidance discourages profiling of minors
Malaysia	No explicit ban; requires lawful purpose and parental consent for minors
Mexico	No explicit ban; express and written consent required; must prioritize best interest of child
New Zealand	No specific legal prohibition
Papua New Guinea	No response available
Peru	No explicit ban; PDPL requires transparency and informed consent
The Republic of the Philippines	No specific legal prohibition
The Russian Federation	No explicit ban; restrictions via sensitive data and purpose limitation principles

Singapore	PDPC Guidelines advise against profiling children for marketing; consent required
Chinese Taipei	No explicit ban; PDPA enforces opt-out and consent for marketing
Thailand	Right to object to direct marketing (Sec. 30); consent required
United States	COPPA (federal) and CDPA (NY) require consent; marketing not 'strictly necessary'
Viet Nam	Prohibited acts under Article 8 of Decree No. 13/ND-CP

The regulatory landscape regarding profiling and targeted advertising for minors in APEC is undergoing a significant shift from a "permissible with consent" model to a "restricted or prohibited" paradigm.

While a comprehensive ban is rare, Indonesia stands out with a strict, explicit prohibition on profiling children under GR 17/2025, setting a high benchmark for protection. Other economies are achieving similar protective outcomes through different legal mechanisms. China effectively prohibits exploitative profiling through its regulations on algorithmic recommendations and addiction prevention. Meanwhile, Canada and Singapore utilize regulatory guidance to establish that profiling children for marketing purposes generally fails to meet the standard for valid or "meaningful" consent, thereby creating a de facto ban for compliant organizations. In jurisdictions like Korea; Thailand; and the United States, while profiling is not legally impossible, the combination of strict parental consent requirements, the right to object to direct marketing, and emerging state-level restrictions (e.g., California) is making the practice increasingly legally risky and practically difficult.

This shifting trend underscores a growing regional consensus that the commercial exploitation of minors' behavioral data is fundamentally incompatible with their developmental best interests. Recognizing this, the primary implication for APEC economies is to consider whether a total or near-total ban on these practices, rather than mere regulation, is necessary to protect vulnerable individuals from manipulative commercialization and algorithmic discrimination.

Section 2. Exploitative and Harmful Use of Children’s Personal Data

I. Introduction

As the use of AI-generated content such as deepfakes grows, so does the risk of children and adolescents being exploited through manipulated images, videos, or voice recordings. These technologies can be used to produce sexual or otherwise harmful content, often without the knowledge or consent of the minor involved.

In addition to deepfake-based abuse, increased digital engagement has heightened children's exposure to harmful or inappropriate content. To address these risks, economies have begun implementing legal frameworks, enforcement mechanisms, and best practices aimed at preventing the misuse of children's personal data for exploitative or harmful purposes.

This section examines notable legislative efforts and regulatory examples designed to protect children and adolescents from such risks, including criminalization of deepfake child sexual abuse material, online safety laws, and platform-specific obligations.

II. Status of APEC economies

1. Australia

The offences in Subdivision 474.D of the Criminal Code capture synthetic child abuse material (such as material generated or modified by AI or animated child abuse material). The Criminal Code defines child abuse material as a person, or representation of a person, who is, or appears to be, under 18 years of age and engaged in, or appearing to be engaged in a sexual pose or activity, or is a victim of torture, cruelty or physical abuse.

In practice, there have been successful prosecutions for AI-generated child abuse material in Australia. In specific, a Tasmanian man was sentenced to two years and eight months in prison for possessing AI-generated child abuse material, following an investigation by the Tasmania Joint Anti Child Exploitation Team (JACET), a partnership between the Australian Federal Police and Tasmania Police. The man had used artificial intelligence to create synthetic child abuse content that depicted children in exploitative scenarios. This case marks a significant enforcement action under Australian law, which criminalizes both real and synthetic child abuse material, emphasizing that AI-generated imagery of this nature is illegal and taken seriously by authorities.

2. Brunei Darussalam

Brunei Darussalam does not currently have explicit legal provisions that specifically address deepfake technology. However, relevant protections are provided under the Children and Young Persons Act, particularly Sections 26 and 27, which prohibit the sexual exploitation of children, the production and distribution of obscene materials involving children, and the exposure of children to harmful content. Although deepfakes are not mentioned by name, these provisions are generally applicable to all forms of child sexual imagery or video content, regardless of the method used to create them. Therefore, any acts involving the creation or dissemination of child sexual abuse material using synthetic or AI-generated content would fall under the scope of these prohibitions.

3. Canada

While PIPEDA does not directly regulate or prohibit the criminal creation or distribution of sexually exploitative deepfake content involving minors, such conduct is addressed under Canada’s Criminal Code. Specifically, Section 163.1 of the Criminal Code prohibits the making, distribution, and possession of child pornography, which includes visual representations that depict or purport to depict minors engaged in explicit sexual activity, regardless of whether the material was generated by artificial intelligence or through other means. In addition, Section 162.1 criminalizes the non-consensual distribution of intimate images, further reinforcing protections against the dissemination of harmful or exploitative visual content involving youth. These provisions serve as the primary legal instruments to combat the creation and spread of deepfake materials that are sexually exploitative or abusive toward children or adolescents.

4. Chile

Chile does not have specific legal provisions that directly address deepfake technology involving children or adolescents. However, the Chilean Criminal Code includes legal provisions regulating child pornography or child sexual abuse material. These provisions prohibit the production, possession, and distribution of sexually exploitative content involving minors. While the law does not explicitly reference synthetic media or deepfake content, the existing criminal regulations concerning child sexual exploitation apply to any material that depicts minors in a sexualized manner, regardless of the method of creation. As such, these laws may be used to address certain cases involving deepfake content if it falls within the scope of child sexual abuse material.

5. People's Republic of China

In the People's Republic of China, while there is no specific legal provision that directly addresses deepfake content involving children or adolescents, several articles under the Law on the Protection of Minors establish obligations and mechanisms to prevent the dissemination of sexually exploitative or harmful content that may include such materials.

Article 77 of the law prohibits cyberbullying that maliciously distorts or damages the image of minors, establishing a duty for network service providers to take appropriate actions when such conduct is identified. Although not explicitly referencing deepfakes, this provision can encompass situations where a minor's image is manipulated in harmful ways using such technology.

Article 79 grants the right to report to either the network service provider or relevant state agencies if online products or services contain information that may be detrimental to a minor's physical or mental well-being. This reporting mechanism provides a route for addressing exposure to harmful content.

Article 80 mandates that if information that could affect a minor's health is discovered, service providers must take specific measures such as issuing warning notices to users, interrupting transmission, deleting or blocking the content, filing reports, and retaining relevant records for inspection by public security authorities.

6. Hong Kong, China

In Hong Kong, China, while there is no dedicated legal framework specifically targeting the creation or dissemination of sexually exploitative or harmful deepfake content involving children or adolescents, certain provisions under existing law offer partial protections. As noted in the response to 7.1, under Data Protection Principle 3 of the Personal Data (Privacy) Ordinance (PDPO), personal data, including that of minors, must not be used for purposes unrelated to the original purpose of collection, such as generating deepfake content, without the data subject's prescribed consent.

In addition, Section 159AAE of the Crimes Ordinance (Cap. 200) criminalizes the act of threatening to distribute deepfake intimate images of any person, including minors, without their consent. This provision applies where the perpetrator intends, or is reckless as to whether, the dissemination would cause humiliation or distress to the individual depicted. Although this offense does not specifically reference children or adolescents, the legal protection it provides applies equally to them.

7. Indonesia

The Law on Sexual Violence Crimes (UU TPKS, Law No. 12 of 2022) provides a robust legal framework addressing digital sexual exploitation. Article 14 of UU TPKS explicitly prohibits the production, transmission, and distribution of electronic documents/information containing sexual violence, which encompasses non-consensual intimate images and deepfakes. Furthermore, the Electronic Information and Transactions Law (UU ITE) criminalizes the distribution of content that violates decency. These laws collectively serve to prosecute the creation and spread of exploitative deepfake content involving minors, treating it as a form of electronic sexual violence.

8. Japan

Japan does not have specific provisions under the Act on the Protection of Personal data (APPI) addressing the creation or dissemination of sexually exploitative or harmful deepfake content involving children or adolescents. However, other individual laws provide relevant protections. In particular, the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children prohibits the possession, production, and distribution of sexual images or videos involving minors under the age of 18. This prohibition extends to synthetic or manipulated content, including deepfakes, that are deemed equivalent to child pornography.

9. Republic of Korea

In Korea, multiple legal frameworks are in place to prevent the creation and dissemination of sexually exploitative or harmful content involving children and adolescents, including deepfake content generated using their personal data. Under Article 44-7 of the Act on Promotion of Information and Communications Network Utilization and Information Protection (the “Network Act”), the distribution of illegal information by any person is prohibited. Related provisions, such as Articles 44-2 and 44-3 of the same Act, grant individuals the right to request the removal of content that infringes upon their privacy or reputation and impose corresponding obligations on information and communications service providers to act on such requests.

Further, the Act on Special Cases Concerning the Punishment of Sexual Crimes (“Sexual Violence Punishment Act”) prohibits the editing, synthesizing, or processing of a person’s image or voice in a manner that may cause sexual humiliation or distress, which may include deepfake content. Under the Telecommunications Business Act, service providers are required to implement measures to prevent the distribution of such edited or synthetic content.

Specifically for minors, the Act on the Protection of Children and Youth Against Sexual Offenses provides enhanced protections. Article 38-2 of the Act enables judicial police officers to request the Korea Communications Standards Commission to delete or block access to child sexual exploitation materials. This reflects Korea’s strengthened legal safeguards against the online sexual exploitation of children and adolescents.

10. Malaysia

In Malaysia, the prevention of sexually exploitative or harmful deepfake content involving children or adolescents is addressed through multiple legal frameworks and coordinated enforcement efforts. While there is no single law that directly references "deepfakes," several statutes collectively serve to prohibit and regulate the creation and dissemination of such harmful materials.

Key among these is the Penal Code (Act 574), which criminalizes the production, possession, and distribution of obscene and exploitative materials, including those involving minors. In addition, the Child Sexual Offences Act 2017 contains provisions that specifically address sexual crimes against children, including offenses related to child pornography and grooming. These provisions can be interpreted to encompass digitally manipulated content, such as deepfakes, that exploit or depict minors in a sexualized manner.

Furthermore, the Communications and Multimedia Act 1998 (CMA) empowers the Malaysian Communications and Multimedia Commission (MCMC) to regulate and take enforcement action against the dissemination of harmful or inappropriate content through digital platforms. The CMA includes provisions to block access to harmful websites and to investigate offenses involving the misuse of online content.

11. Mexico

In Mexico, while data protection laws do not contain specific provisions directly addressing the creation or dissemination of sexually exploitative or harmful deepfake content involving children or adolescents, various other legal frameworks provide substantial safeguards in this area. Under Article 77 of the General Law on the Rights of Children and Adolescents (LGDNNA), the processing, whether direct or indirect, of a minor’s image, name, personal data, or any identifying reference that could damage their honor or reputation, infringe upon their rights, or expose them to risk, is considered a violation of their privacy.

Moreover, such harmful content is criminalized under Mexico’s Federal Criminal Code, which prohibits child pornography and various forms of sexual exploitation. These provisions are further reinforced by recent legislative reforms targeting digital violence and cybercrimes related to sexual privacy, collectively referred to as the “Olimpia Law.” These reforms expand criminal liability to include the non-consensual distribution of intimate content, including synthetic or manipulated media such as deepfakes.

Together, these legal instruments, spanning child protection, criminal law, and cybercrime legislation, form a comprehensive framework that functions to prevent and penalize the creation and spread of sexually exploitative or harmful deepfake content involving minors, despite the absence of direct regulation under Mexico’s data protection statutes.

12. New Zealand

New Zealand addresses the creation and dissemination of sexually exploitative or harmful digital content involving children and adolescents through the Harmful Digital Communications Act 2015. The primary objective of this Act is to deter, prevent, and mitigate harm caused by digital communications to individuals, including minors. The legislation establishes mechanisms to provide victims, such as children and young people, with a swift and effective means of redress when they are targeted by harmful digital content. Although the Act does not specifically reference deepfake technology, its scope extends to all forms of digital communications, which includes online deepfake content. As such, sexually

exploitative or harmful deepfakes involving minors may fall within the ambit of this legislation, allowing affected individuals to seek remedies through the processes it provides.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

In Peru, while the Personal Data Protection Law (PDPL) does not contain specific provisions directly addressing the prevention of sexually exploitative or harmful content—such as deepfake materials involving children or adolescents—other legal frameworks provide mechanisms to address such issues. Notably, the Peruvian Criminal Code and Law No. 32314 establish criminal liability for acts involving the misuse of personal data, including scenarios that may involve the unauthorized creation or dissemination of harmful digital content.

Therefore, while PDPL itself is limited in scope regarding sexually exploitative or harmful digital content, Peru’s broader criminal and child protection laws serve as the primary legal instruments for addressing these risks.

15. The Republic of the Philippines

Under Republic Act No. 11930, known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act, the Philippines has established a legal framework that addresses harmful digital content involving minors, including deepfakes. Specifically, Section 4 of the Act criminalizes the production, possession, access, and distribution of materials that sexually exploit children, regardless of whether such materials are real or digitally altered.

16. The Russian Federation

In Russia, while there is no law specifically targeting deepfake technology, the creation and dissemination of sexually exploitative or harmful content involving children or adolescents, including content that may involve the misuse of personal data (such as deepfakes), is addressed through a combination of legal instruments. Notably, Federal Law No. 436-FZ on Protecting Children from Information Harmful to Their Health and Development prohibits the distribution of harmful content to minors, including pornography and materials promoting violence or self-harm. In addition, the Russian Criminal Code criminalizes the production, dissemination, and possession of child pornography and other forms of sexual exploitation involving minors.

17. Singapore

Singapore has strengthened its regulatory framework with the Online Safety (Miscellaneous Amendments) Act 2022, which amended the Broadcasting Act. This Act empowers the Infocomm Media Development Authority (IMDA) to issue directions to online communication services to disable access to "egregious content," which explicitly includes content

advocating or depicting sexual violence and child sexual exploitation. Additionally, the Penal Code (Section 377BB and 377BC) criminalizes voyeurism and the distribution of intimate images without consent, which covers the dissemination of deepfake sexual imagery.

18. Chinese Taipei

In Chinese Taipei, Article 46-1 of the Protection of Children and Youths Welfare and Rights Act (1992) prohibits children and adolescents from being exposed to content that may cause physical or psychological harm. This provision aims to prevent the dissemination and exposure of harmful materials, including sexually exploitative or abusive deepfake content involving minors. The responsibility for enforcing this regulation falls on internet platforms and service providers, which are expected to prevent the distribution and accessibility of such content through their services. However, the regulatory approach under this law is primarily based on self-regulation.

19. Thailand

Thailand addresses harmful digital content through the Computer Crime Act (CCA) B.E. 2560 (2017). Section 14(4) of the CCA prohibits the importation of data of a pornographic nature into a computer system that is accessible to the public. Additionally, the Criminal Code (Section 287) criminalizes the production and distribution of obscene materials. These laws are technologically neutral and are applied to prosecute the creation and spread of AI-generated child sexual abuse material (CSAM).

20. United States

In the United States, there are specific laws to address the dissemination of sexually exploitative or harmful deepfake content involving children and adolescents. At the federal level, the Tools to Address Known Exploitation by Immobilizing Technological Deep Fakes on Websites and Networks Act (TAKE IT DOWN Act) was enacted in May 2025. This law prohibits the distribution of non-consensual intimate visual depictions generated by artificial intelligence, including such images involving minors. The legislation aims to provide a mechanism for the removal of AI-generated intimate content that was created and shared without the subject's consent.

For example, California enacted Assembly Bill 1831 (AB 1831) in September 2024 at the state level. This law prohibits the creation, possession, and distribution of child sexual abuse material (CSAM) generated by AI. The legislation extends existing protections against CSAM to include synthetically generated content, closing a gap in prior statutory definitions that did not explicitly cover AI-generated images. These legal developments reflect a growing recognition of the threats posed by emerging technologies to the privacy and safety of minors and seek to enhance regulatory tools for preventing such digital exploitation.

21. Viet Nam

Viet Nam’s regulatory framework includes certain general provisions aimed at protecting children from harmful digital content, including sexually exploitative materials. Article 6 of Decree No. 13/2023/ND-CP on Children establishes protections for children’s rights and

well-being. However, there are currently no specific legal provisions that directly address the creation or dissemination of harmful deepfake content involving children or adolescents.

III. Comparative Analysis and Implication

The following table presents a comparative analysis of the legal and regulatory measures across APEC economies to prevent the exploitative and harmful use of children's personal data, including deepfake-based sexual content.

Table 22 Exploitative and Harmful Use of Children's Personal Data

Economy	Deepfake Law Coverage Summary
Australia	Criminal Code covers synthetic child abuse material; AI-generated content prosecuted
Brunei Darussalam	Children and Young Persons Act indirectly covers AI-generated abuse
Canada	Criminal Code prohibits child porn including synthetic media; NCII also criminalized
Chile	Child pornography laws apply; not specific to deepfakes
People's Republic of China	Minors Protection Law covers image manipulation and harmful content; not deepfake-specific
Hong Kong, China	Crimes Ordinance criminalizes threat to distribute deepfake intimate images
Indonesia	Sexual Violence Crime Law (UU TPKS) covers electronic sexual violence/deepfakes
Japan	Child pornography laws extend to synthetic images
Republic of Korea	Multiple acts prohibit illegal distribution, image editing; strong protection for minors
Malaysia	Penal Code, CSA 2017, and CMA regulate harmful materials incl. deepfakes
Mexico	Child protection and criminal law (Olimpia Law) prohibit harmful synthetic content
New Zealand	Harmful Digital Communications Act covers all digital content incl. deepfakes
Papua New Guinea	No information available
Peru	Criminal Code and Law No. 32314 address misuse of personal data; not deepfake-specific
The Republic of the Philippines	OSAEC Act criminalizes deepfake child sexual abuse material
The Russian Federation	Law 436-FZ and Criminal Code prohibit harmful/sexual content incl. AI-generated
Singapore	Online Safety Act & Penal Code cover egregious content and non-consensual images

Chinese Taipei	Protection of Children Act Article 46-1 bans harmful exposure; self-regulation model
Thailand	Computer Crime Act prohibits pornographic computer data
United States	TAKE IT DOWN Act & CA AB1831 prohibit AI-generated CSAM/nonconsensual intimate visual depictions
Viet Nam	General child protection laws apply; no deepfake-specific law

The review of legal frameworks across APEC economies highlights a critical transition from relying on general criminal statutes to adopting specific measures targeting AI-generated exploitation. Currently, most jurisdictions address deepfake abuse by interpreting existing, technologically neutral laws to encompass synthetic media. However, an increasing number of economies are enacting targeted legislation to explicitly criminalize the unauthorized creation and distribution of synthetic intimate content, effectively closing legal loopholes regarding the distinction between 'real' and 'fake' imagery. Beyond criminalization, there is a notable shift toward a more holistic safety framework; regulators are increasingly prioritizing the rapid removal of harmful content and holding digital platforms accountable. This signals a growing recognition that protecting minors from digital sexual violence requires not only punitive measures but also proactive safeguards to preempt the dissemination of exploitative material.

The key implication of this shift is the urgent necessity for APEC economies to establish strict criminal and civil penalties specifically targeting the creation and non-consensual distribution of deepfake-based sexual content involving minors. To be effective, this requires a dedicated legal framework that acknowledges the unique and profound harm of synthetic abuse, thereby facilitating rapid takedown procedures and mandatory notifications to law enforcement. To complement these legal responses, policymakers must also mandate the adoption of data provenance and watermarking technologies, enabling platforms to trace the origins of synthetic media. Ultimately, the framework should impose strict liability on platforms that fail to implement effective content filtering and reporting mechanisms, ensuring that technological innovation is matched by robust institutional accountability.

Section 3. Legal Mechanisms Enabling Children and Adolescents to Request the Takedown of Online Content

I. Introduction

Children and adolescents increasingly create and share content online, often without full awareness of its long-term implications. As they mature, the desire to remove content shared during earlier stages of life, including images, posts, or videos that may be embarrassing, harmful, or privacy-intrusive, becomes more pressing.

Recognizing this need, some jurisdictions have introduced legal mechanisms or institutional programs enabling minors (or their guardians) to request the takedown of online content. These mechanisms are often referred to as part of the “right to erasure” or “right to be forgotten” and may be implemented through statutory rights, self-regulatory industry practices, or government-supported initiatives.

This section explores whether such takedown rights are formally recognized, how they are exercised in practice, and highlights best practices and exemplary models that aim to empower minors in managing their digital footprint.

II. Status of APEC economies

1. Australia

As of now, there is no specific statutory right under Australian law that explicitly grants children or adolescents the right to request the takedown of harmful content such as deepfake or sexually exploitative material involving them. However, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA)—which oversees policy and legislation in the areas of communications and online safety—may provide further guidance or coordination in this domain.

2. Brunei Darussalam

Brunei Darussalam does not have a specific statutory "takedown right" for minors. However, the Content Advisory Council (under the Authority for Info-communications Technology Industry, AITI) accepts complaints regarding offensive or harmful online content. While this is an administrative mechanism rather than a guaranteed legal right for the child, it provides a practical avenue for requesting the removal of content that violates local content standards, including child exploitation material.

3. Canada

In Canada, while children and adolescents are not granted a formal “right to erasure” under privacy legislation such as the Personal Data Protection and Electronic Documents Act (PIPEDA), they can request the takedown of sexually exploitative or harmful deepfake content involving them. This is because such content is deemed illegal under the Criminal Code, specifically Sections 163.1 (which addresses child pornography offenses) and 162.1 (which concerns non-consensual distribution of intimate images). These provisions criminalize the creation, possession, and distribution of exploitative or intimate images of minors, including those generated through artificial means such as deepfakes. Consequently, victims or their representatives can report such content to law enforcement or online platforms, which are legally required to act to remove the material.

4. Chile

In Chile, there is no specific law granting children or adolescents a formal right to request the takedown of harmful content. However, under Article 20 of the Chilean Constitution, individuals, including minors, may seek judicial relief through a legal remedy known as the recurso de protección. This mechanism allows anyone whose constitutional rights are being violated to petition the courts for immediate protection. In practice, this remedy has been used to request the removal of online content that infringes on privacy or other fundamental rights. While the recurso de protección is not tailored exclusively to children or adolescents,

it provides a general legal avenue through which they—or their legal representatives—can request takedown of harmful or exploitative content involving them.

5. People's Republic of China

China has established a strong legal framework for content takedown involving minors. Article 80 of the Law on the Protection of Minors explicitly mandates that network service providers must prompt measures—such as deleting, blocking, or disconnecting links—upon discovering or receiving reports of information that may harm the physical or mental health of minors. Additionally, the Provisions on the Cyber Protection of Children's Personal Information (Article 20) grant guardians the specific right to request the deletion of a child's personal information if it was collected or used in violation of laws or agreements.

6. Hong Kong, China

In Hong Kong, China, children and adolescents do not have a standalone statutory right to request the takedown of harmful content. However, under the Personal Data (Privacy) Ordinance (PDPO), if the content in question constitutes "doxxing", defined as the unlawful disclosure of personal data without consent with an intent to cause harm, the Privacy Commissioner for Personal Data has the authority to intervene. Specifically, the Commissioner may issue a cessation notice to the relevant online platform, requiring the removal or restriction of access to the harmful content.

While not a personal takedown right per se, it provides a practical avenue through which harmful content involving children or adolescents may be removed from online platforms, particularly in cases involving harassment or the unauthorized use of personal data.

7. Indonesia

Indonesia provides a takedown mechanism through the Electronic Information and Transactions Law (UU ITE). Specifically, electronic system providers are obligated to take down prohibited content (including child pornography and content violating decency) within 24 hours of being notified (or 4 hours for urgent cases).

8. Japan

In Japan, children and adolescents do not have a distinct statutory "right to erasure" or "takedown right" under the APPI. However, if harmful content involving minors includes their personal data that qualifies as "retained personal data" under Article 16, Paragraph 4 of the Act on the Protection of Personal data (APPI), a data subject—such as the minor or their legal representative—may submit a "request to suspend use" of such data in accordance with Article 35, Paragraph 1. This legal mechanism allows individuals to seek cessation of use or deletion of their retained personal data when it has been handled in violation of statutory provisions, including being collected or used beyond the scope of its intended purpose.

9. Republic of Korea

In Korea, there is no specific legal mechanism that grants children or adolescents a distinct “right to request takedown” of harmful content. However, general provisions under the Act on Promotion of Information and Communications Network Utilization and Information Protection (the “Network Act”) provide a basis for takedown requests.

Specifically, Article 44-2 of the Network Act allows individuals who believe their rights, such as privacy or reputation, have been infringed upon by online content to request the deletion or correction of such content. In response, Article 44-3 mandates that information and communications service providers implement provisional measures, such as temporary blocking, while the matter is under review. These provisions apply universally and are not tailored exclusively to minors, but they can be used to seek the removal of harmful content involving children or adolescents when relevant.

10. Malaysia

In Malaysia, while there is no explicit statutory provision granting children or adolescents a standalone right to request the takedown of harmful content, including deepfakes, a practical mechanism exists through the Malaysian Communications and Multimedia Commission (MCMC). Under the Communications and Multimedia Act 1998 (CMA), the MCMC has the authority to investigate and act upon complaints related to offensive, indecent, or harmful content disseminated online.

If harmful content involving children or adolescents—such as sexually exploitative or manipulated materials—is identified, individuals, including the affected minors or their guardians, may submit a complaint directly to the MCMC. Upon review, the MCMC can instruct internet service providers and platform operators to block access to or remove such content from digital platforms.

11. Mexico

In Mexico, while the general data protection framework, particularly under the Federal Law on the Protection of Personal Data Held by Private Parties, establishes the right to cancel personal data (a component of the ARCO rights: Access, Rectification, Cancellation, and Opposition), the specific protections related to takedown of harmful content involving children or adolescents are primarily found in specialized legal regimes and judicial interpretations. These frameworks supplement the general right to erasure by incorporating heightened safeguards for minors as a vulnerable group.

Importantly, Mexican jurisprudence has played a central role in operationalizing these protections. The Supreme Court of Justice has consistently emphasized the constitutional principle of the "best interests of the child" in adjudicating cases involving minors’ digital rights. In a recent example, the Court ordered the cancellation of data processing activities involving a minor, recognizing the necessity of removing such harmful content to protect the child’s dignity and privacy. This case affirms the judiciary’s commitment to reinforcing children's rights to request the takedown of personal data, especially when such data may be linked to reputational or psychological harm.

12. New Zealand

In New Zealand, there is no formal or statutory right granted specifically to children or adolescents to request the takedown of harmful online content. However, Netsafe, the

designated agency under the Harmful Digital Communications Act 2015, provides practical support to victims of harmful digital communications, including minors. This support includes working with online platforms or content hosts to seek voluntary removal of harmful material where possible. Additionally, the District Court holds the authority to issue binding and enforceable orders requiring the takedown or disabling of harmful digital content. While not a right exercised directly by minors, these mechanisms collectively offer avenues for removing damaging material involving children or adolescents from online platforms.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

Under Peru's Personal Data Protection Law (PDPL), individuals—regardless of age—are granted the right to deletion (derecho de supresión), which allows data subjects to request the removal of their personal data when it is no longer necessary, when consent has been withdrawn, or when the data is being processed unlawfully. This right is applicable to children and adolescents as data subjects, either directly or through their legal representatives.

In practice, while the PDPL does not establish a separate or explicit takedown mechanism specifically for minors or for harmful content like deepfakes or exploitation material, the general framework of the right to deletion offers a legal basis for such requests.

15. The Republic of the Philippines

Yes. Under Section 9 of Republic Act No. 11930 (Anti-OSAEC and Anti-CSAEM Act), children or adolescents, or their representatives, are granted protection through obligations imposed on Internet Intermediaries. These intermediaries are required to immediately block access to, remove, or take down any internet address, URL, or online platform that contains online sexual abuse or exploitation of children (OSAEC) or child sexual abuse or exploitation materials (CSAEM) upon notice by authorities or relevant agencies.

16. The Russian Federation

In Russia, while there is no specific provision labeled as a "takedown right" for children or adolescents, individuals, including minors through their legal representatives, may effectively exercise such rights under Federal Law No. 152-FZ on Personal Data. This law provides data subjects with the right to request the deletion, blocking, or correction of their personal data if the data is inaccurate, unlawfully obtained, or no longer necessary for the stated processing purposes. These provisions establish a practical mechanism for requesting the removal of harmful or unlawfully processed content involving children's or adolescents' personal data. As such, although not framed as a child-specific takedown regime, the law allows for the substantive enforcement of content removal when children's personal data is involved.

17. Singapore

Under the Broadcasting Act 1994, IMDA can issue directions to online communication services to disable access to "egregious content" (including child sexual exploitation material) for Singapore users. This effectively functions as a takedown mechanism for the most harmful content involving minors as access to the egregious content will be disabled by the online communication service for Singapore users.

18. Chinese Taipei

Child and Youth Sexual Exploitation Prevention Act requires internet platform providers to remove or block access to web pages containing content related to child and youth sexual exploitation upon notification by the police or competent authorities. Providers must also retain data for investigation.

19. Thailand

Thailand provides a takedown mechanism under the Computer Crime Act (CCA). The MDES can seek a court order to block or remove computer data that is illegal (e.g., pornography, threats to domestic security) or harmful. Additionally, under the PDPA, data subjects have the right to request erasure, and data controllers must comply unless there is a legal ground for retention.

20. United States

In the United States, minors can request the takedown of harmful or unwanted digital content involving their personal data. At the federal level, the TAKE IT DOWN Act, enacted in 2025, establishes a mechanism that allows minors (or their authorized representatives) to submit requests for the removal of non-consensual intimate visual depictions, including content generated by artificial intelligence. A centralized system managed by the National Center for Missing and Exploited Children (NCMEC) enables affected individuals to report and request takedown of such content, offering a streamlined avenue for content removal.

At the state level, California's Eraser Law provides individuals under the age of 18 with the right to delete or request deletion of content they have posted on websites, mobile apps, or other online services. The law applies to content that minors themselves have uploaded or shared, and it requires operators of services directed to minors—or that knowingly have minor users—to provide a mechanism for deletion upon request.

21. Viet Nam

Under Viet Nam’s current legal framework, children and adolescents, like any other individuals, have the right to request the removal of harmful content. This general right is not specifically codified for minors, but it is recognized as part of broader data protection and child rights regulations. While there is no dedicated mechanism or law granting children a unique or formal “takedown” right, existing laws allow individuals to seek the deletion or blocking of personal data or content that infringes upon their rights, including harmful materials.

III. Comparative Analysis and Implication

The following table presents a comparative analysis of the legal and practical frameworks across APEC economies concerning the takedown rights for content involving children and adolescents.

Table 23 Legal Mechanisms Enabling Children and Adolescents to Request the Takedown of Online Content

Economy	Takedown Right	Legal/Practical Framework
Australia	No explicit statutory right	Departmental guidance possible (DITRDCA)
Brunei Darussalam	Admin Mechanism	Content Advisory Council (AITI) complaints process
Canada	Yes (via Criminal Code)	Section 163.1 (child pornography), Section 162.1 (non-consensual intimate images)
Chile	Yes (general remedy)	Recurso de proteccion under Article 20 of Constitution
People's Republic of China	Yes (Explicit for Minors)	Law on Protection of Minors (Art. 80); Cyber Protection Provisions (Art. 20)
Hong Kong, China	Partial (not personal right)	PDPO Commissioner may issue cessation notice for doxxing
Indonesia	Yes	UU ITE
Japan	Conditional	APPI Article 35(1) – Request to suspend use of personal data
Republic of Korea	Yes (general right)	Network Act Articles 44-2, 44-3
Malaysia	Yes (practical mechanism)	Complaints to MCMC for content removal under CMA
Mexico	Yes (with judicial support)	ARCO rights + jurisprudence on the child of the best interests
New Zealand	Yes (via agency/court)	Netsafe (Harmful Digital Comms Act), District Court orders
Papua New Guinea	Enforcement Mechanism	Cybercrime Code Act (Authority-ordered removal)
Peru	Yes (general right)	
The Republic of the Philippines	Yes (explicitly for minors)	RA No. 11930 Section 9 Obligations on intermediaries
The Russian Federation	Yes (general mechanism)	152-FZ deletion/blocking upon request
Singapore	Yes	Broadcasting Act 1994 (IMDA directions for egregious content)
Chinese Taipei	Yes	Child and Youth Sexual Exploitation Prevention Act (Art. 8)
Thailand	Yes	Computer Crime Act (Court-ordered blocking); PDPA Erasure Right

United States	Yes (federal and state laws)	TAKE IT DOWN Act (2025), California Eraser Law
Viet Nam	Yes (general framework)	Decree 13/2023 – general removal rights apply to all

The review of takedown rights across APEC economies reveals a diverse but strengthening ecosystem of mechanisms to remove harmful content involving minors.

While few jurisdictions grant a "Takedown Right" as a standalone, child-specific statutory power exercised directly by the minor against a platform, almost all economies have established functional equivalents through one of three approaches: (1) Data Protection Rights, where general rights to erasure or suspension of use (e.g., Japan; Peru; Thailand) are leveraged; (2) Cyber-Safety Regulation, where specialized agencies like Australia's eSafety Commissioner or Malaysia's MCMC are empowered to order takedowns of harmful content; and (3) Criminal/Intermediary Liability Laws, where platforms are legally obligated to remove illegal content such as CSAM or non-consensual intimate images upon notice (e.g., the Philippines; Singapore; Chinese Taipei). The most advanced frameworks, such as in Australia and China, provide clear, expedited administrative paths specifically designed to protect minors from digital harm, moving beyond slow judicial processes to offer rapid relief.

This landscape indicates a shift from viewing takedowns solely as a privacy issue to treating them as a critical safety intervention, with regulators increasingly prioritizing rapid, authority-driven removal mechanisms to minimize the duration of harm for minors.

Chapter 9 Self-Regulation by Companies and Government Support (Incentives, etc.) Regarding Children or Adolescents' Personal Data Protection

I. Introduction

While legislation sets the minimum floor for compliance, self-regulation and government incentives drive the "race to the top." In the rapidly evolving digital landscape, statutory laws often struggle to keep pace with new technologies. Self-regulatory mechanisms—such as industry codes of conduct, trustmarks, and voluntary corporate policies—allow the private sector to implement agile, child-centric protections that go beyond legal requirements.

Furthermore, government support in the form of certification schemes (Safe Harbors), financial incentives, or public-private partnerships is crucial. These measures encourage companies not just to comply with the law, but to proactively invest in safer digital environments for minors. This section explores how APEC economies are utilizing these soft-law mechanisms to enhance the ecosystem of protection.

II. Status of APEC economies

1. Australia

Australia utilizes a co-regulatory model involving industry codes. Under the Online Safety Act 2021, industry associations developed the "Consolidated Industry Codes of Practice for the Online Industry," which were registered by the eSafety Commissioner in 2023. These codes require platforms to take proactive steps to minimize harms to children (e.g., restricted access to mature content). Additionally, the Office of the OAIC encourages the development of APP Codes, which are binding on the industry once registered.

2. Brunei Darussalam

No information was found in relation to this issue.

3. Canada

There are voluntary self-regulatory initiatives by companies in Canada aimed at protecting children's and adolescents' personal data, but these are largely industry-driven and not specifically supported by direct government incentives or financial assistance.

4. Chile

While currently limited, the PDPL explicitly promotes the adoption of "Privacy Management Programs" and certification models. This creates a legal framework where the future Data Protection Agency will certify compliance models, effectively incentivizing self-regulation.

5. People’s Republic of China

Self-regulation is a key component of China's governance model. The Internet Society of China (ISC) has issued the "Convention on the Self-Discipline of the Internet Industry," which includes pledges to protect minors. Major technology companies (e.g., Tencent, Douyin) voluntarily implemented "Youth Modes" and time limits for minors before they became mandatory, often acting under "administrative guidance." These corporate initiatives are heavily supported by state media and regulators as exemplary practices.

6. Hong Kong, China

Companies are increasingly enabling greater parental participation in order to protect the personal data of children or adolescents. This includes allowing parents to manage and monitor their children’s online activities through the use of “parental control” features.

7. Indonesia

Industry associations play a role in self-regulation. The Indonesian Fintech Association (AFTECH) enforces a Code of Conduct regarding data privacy for its members, which includes protecting vulnerable consumers. While not child-specific, these industry standards fill gaps where detailed regulations are still being implemented.

8. Japan

Japan has a highly developed system of government-supported self-regulation known as "Accredited Personal Information Protection Organizations". The PPC accredits private organizations to handle complaints and establish guidelines for their member companies. Furthermore, the "PrivacyMark" system, operated by JIPDEC, is a widely recognized certification that incentivizes companies to maintain high privacy standards. Obtaining this mark is a significant commercial incentive for consumer trust.

9. Republic of Korea

There is no government-established system to support voluntary regulation by companies.

However, some internet platform companies have voluntarily developed and are implementing special protection policies for children and adolescents. For example, Naver is running the “Green Internet” campaign to provide special protection for children and adolescents. Specifically, the campaign includes minimizing exposure to harmful posts through age restriction features, managing sexual-related keywords and search terms harmful to those under 19 as youth-harmful search terms, mandating age restrictions on live broadcasts or videos containing adult themes in their content guidelines, and operating a dedicated monitoring team and emergency reporting center.

10. Malaysia

Under Act 709, there are no specific voluntary self-regulatory initiatives mandated by the government to protect children's or adolescents' personal data.

11. Mexico

To date, there is no specific knowledge of voluntary self-regulatory initiatives by companies exclusively aimed at protecting the personal data of children or adolescents in Mexico. However, data protection legislation provides for the existence of self-regulation schemes as complementary tools to ensure legal compliance.

Both the LFPDPPP and the LGPDPPSO promote these efforts as mechanisms that can enhance accountability, offer legal incentives, and help demonstrate compliance to the supervisory authorities.

12. New Zealand

The Marketing Association of New Zealand maintains a Code of Practice regarding marketing to children and young people, which includes data privacy considerations. This is a voluntary industry standard that complements the Privacy Act.

13. Papua New Guinea

No information was found in relation to this issue.

14. Peru

The Interactive Advertising Bureau (IAB) Peru promotes self-regulatory guidelines for digital marketing, which includes ethical standards for data collection involving minors, although these are not government-enforced.

15. The Republic of the Philippines

Some companies in the Philippines have child safety and children’s privacy programs and initiatives.

For the National Privacy Commission, its Kabataang Digital (Digital Youth) program has partnered with private companies in their information and awareness materials and campaigns. The KD campaign actively collaborates with government agencies, private sector organizations, and industry leaders to enhance its impact and reach.

16. The Russian Federation

Roskomnadzor (Federal Service for Supervision of Communications, Information Technologies and Mass Media) provides guidelines for companies and indirectly encourages self-regulation.

The Code of Ethics for the Internet Industry by RAEC (Russian Association for Electronic Communications) includes commitments to protect minors from harmful content, implement an age rating system, and provide users with tools to restrict access to unwanted content.

The Guidelines for the Protection of Children on the Internet recommend using simple and clear language in terms of service and privacy policies to help both children and their parents understand the content.

17. Singapore

Singapore employs a strong government-incentivized model through the "Data Protection Trustmark (DPTM)." The Data Protection Trustmark (DPTM) is a voluntary enterprise-wide certification for organizations to demonstrate accountable data protection practices. Additionally, the "Digital for Life" movement is a government-supported community initiative where private companies contribute resources to educate children on digital safety.

18. Chinese Taipei

The Institute of Watch Internet Network (iWIN) is a government-supported multi-stakeholder organization that coordinates self-regulation among internet platform providers to prevent harmful content and protect children's privacy. Industry members adhere to iWIN’s codes to avoid direct regulatory intervention.

19. Thailand

No information was found in relation to this issue.

20. United States

There are self-regulatory codes of conduct prohibit personalized advertising targeted at children under the age of 13 without parental consent. Such codes may serve as industry standards. The Global CBPR Forum recently adopted new Global CBPR System Program Requirements to increase accountability for processing children’s data. Through the United States’ participation in the Global CBPR Forum, United States companies can certify to the Global CBPR System, a voluntary, multilateral data privacy certification for companies to demonstrate compliance with government-recognized requirements

21. Viet Nam

Decree No. 13/ND-CP includes provisions encouraging agencies, organizations, and individuals to apply personal data protection standards appropriate to their respective sectors, industries, and activities involving the processing of personal data.

III. Comparative Analysis and Implications

The following table presents a comparative analysis across APEC economies concerning the role of self-regulation by companies and government support (incentives, etc.) in protecting children's and adolescents' personal data.

Table 24 Self-Regulation

APEC Economy	Voluntary Self-Regulation / Industry Initiatives
Australia	Yes - Registered Industry Codes under Online Safety Act
Brunei Darussalam	No information found
Canada	Yes – industry-led, no gov’t incentives
Chile	Yes - PMP
People’s Republic of China	Yes – ISC Self Discipline
Hong Kong, China	Yes – parental controls increasingly adopted
Indonesia	Yes – Fintech Codes
Japan	Yes – JIPDEC PrivacyMark
Republic of Korea	Yes – e.g., Naver Green Internet campaign
Malaysia	No government mandate
Mexico	Self-regulation promoted as compliance tool
New Zealand	Yes – Marketing Code
Papua New Guinea	No information found
Peru	Yes – IAB Standards
The Republic of the Philippines	Yes – NPC + private sector programs
The Russian Federation	Yes – Roskomnadzor & RAEC Code of Ethics
Singapore	Yes – DPTM certification
Chinese Taipei	Yes – iWIN
Thailand	No information found
United States	Yes
Viet Nam	Encouraged by Decree 13/ND-CP

The comparative analysis of self-regulation across APEC economies reveals a significant evolution from isolated corporate social responsibility initiatives toward structured "co-regulatory" ecosystems. While statutory laws provide the necessary compliance baseline, APEC economies are increasingly relying on flexible, government-supported mechanisms to bridge the gap between rigid regulations and rapidly evolving digital risks. Three distinct models of government-industry collaboration have emerged from this shift. First, the "Incentive-Based Model," utilized in Japan and the United States, grants legal benefits or

market-differentiating certifications to companies that voluntarily adopt higher standards. Second, the "State-Guided Co-Regulation Model," seen in Australia; China; and Malaysia, involves industry codes developed by the private sector that gain statutory force through formal registration with regulators. Third, the "Multi-Stakeholder Model," exemplified by Chinese Taipei's iWIN, leverages government-backed NGOs to coordinate industry actions without direct, heavy-handed intervention.

These findings seem to indicate that effective protection should include efforts beyond legislation alone. The most successful jurisdictions are those that actively foster a compliance ecosystem by using financial grants, liability protections, and official accreditation to motivate the private sector. Building on this insight, government efforts should prioritize a "mandate-and-incentivize" approach. While regulation must establish a non-negotiable minimum baseline—such as the prohibition of targeted advertising and the requirement for granular consent—incentives like tax breaks or fast-track certifications should be offered to companies that exceed these minimums, particularly those developing innovative, privacy-enhancing technologies. To further solidify this ecosystem, APEC economies can establish a harmonized regional certification mark for child-safe online services. By leveraging government support to build trusted third-party auditing bodies for such certifications, regulators can provide clear signals to parents and consumers while ensuring that privacy protections remain agile enough to address emerging threats, such as AI and deepfakes, likely more effectively than the legislative cycle alone allows.

Chapter 10 Conclusion

This study provides the first comprehensive, cross-economy analysis of legal frameworks, enforcement systems, age-assurance practices, privacy-by-design implementation, and public perception regarding the protection of children's and adolescents' personal data across the 21 APEC member economies. The findings reveal that, while economies share a common recognition of the need to protect minors in digital environments, the approaches vary widely across jurisdictions. Some economies, such as China; Indonesia; Korea; and Viet Nam, have enacted explicit statutory provisions for minors, including specific age thresholds and guardian-consent requirements. Others rely on general privacy laws, sectoral regulation, or child-protection legislation to address issues related to digital privacy, resulting in fragmented governance structures.

The analysis further demonstrates that service providers—particularly those operating across borders—face practical difficulties in navigating divergent rules on guardian consent, age thresholds, enforcement mechanisms, and notice obligations. Although several economies impose child-specific consent requirements, most do not differentiate penalties or enforcement levels between violations involving adults and those involving minors, creating uncertainty for organizations in determining risk exposure. Only a minority of economies adopt enhanced sanctioning standards or detailed guardian-verification procedures. These findings underscore the need for clearer, more interoperable approaches to children's data protection across the region.

Transparency obligations similarly vary across APEC. While some economies require age-appropriate notices using simple, accessible language, many apply only general notice

requirements, leaving practical gaps in communicating privacy information to minors. Even in economies where age-appropriate notices are encouraged, actual implementation remains inconsistent. Survey results reinforce these findings: respondents overwhelmingly perceived privacy notices as insufficient and difficult for minors to understand. These observations indicate a continued need for concrete guidance to support effective, child-centered transparency practices in digital services.

With respect to Privacy by Design (PbD), only a few APEC economies codify PbD principles in legislation. Nevertheless, the underlying concept is broadly recognized and partially reflected in domestic guidelines, sectoral rules, and voluntary corporate practices. In particular, some economies identify higher-risk processing—such as profiling, geolocation, or targeted content delivery—as requiring more stringent protective measures. Despite these convergences, however, implementation remains uneven, suggesting value in developing practical, interoperable approaches to PbD that respond to risks faced by children and adolescents in digital settings.

Age-assurance mechanisms represent another area of divergence. Very few economies mandate general age verification, while those with requirements typically limit them to specific regulated sectors such as alcohol, gambling, or explicit content. The methods employed also differ considerably, ranging from government ID verification and mobile authentication to biometric checks and AI-based estimations. In light of these findings, continued dialogue and efforts should be pursued to explore age-assurance mechanisms that take into account risk-proportionate approaches and the principle of data minimization, in order to support safer digital environments for children and adolescents.

The study also highlights important questions regarding minors' rights, including the right to access, correction, erasure, and objection. Although these rights are recognized across most economies, the relationship between minors' rights and parental or guardian authority differs widely. Some economies allow parents to exercise rights exclusively on behalf of young children; others apply capacity-based tests, particularly for older adolescents. These differing models illustrate the likely importance of further dialogue on evolving capacities, representational authority, and mechanisms that best protect minors while respecting their growing autonomy.

Finally, the analysis reveals that issues such as profiling, targeted marketing, and harmful content—particularly deepfake-based exploitation—are not comprehensively addressed through privacy legislation in most economies. Instead, such harms are often governed by criminal law, cybercrime statutes, or media-specific regulation. While takedown mechanisms exist in many jurisdictions, their legal foundations and scope vary, ranging from formal statutory remedies to enforcement-based practices. Survey respondents expressed exceptionally strong concern about deepfake harms, confirming the importance of continuing regional dialogue on safeguards that address both privacy and safety dimensions.

While there are many divergences, there are also areas of convergence across APEC economies with respect to parental consent requirements. The survey shows that, in most economies, where consent is required for the processing of children's personal data,

consent obtained from a parent or legal guardian is typically required. Furthermore, in a limited number of economies, the scope of individuals permitted to provide consent is defined more broadly, extending beyond parents or legal guardians under specific circumstances.

Taken together, these findings suggest that while APEC economies share a commitment to enhancing the digital safety and privacy of children and adolescents, meaningful gaps remain in regulatory clarity, interoperability, and practical implementation. Strengthening cooperation across the region—through shared principles, common understandings, and coordinated capacity building—will support the development of robust, future-ready frameworks that reflect the best interests of children and adolescents.

Based on the comprehensive comparative analysis and the findings from the APEC workshop, the following section outlines the **Key Outcomes and The Way Forward**. This section presents a set of recommendations for APEC and its member economies, structured around a shared vision, strategic policy directions, actionable tasks, and a roadmap for implementation.

Key Outcomes and The Way Forward: Recommendations for APEC

To foster a safer, more trusted, and child-appropriate digital ecosystem, it is recommended that APEC and its member economies adopt a structured approach driven by the following framework:

1. Vision and Principles

APEC member economies should seek to establish a unified goal grounded in shared understanding. We recommend setting **"Acknowledging Different Approaches"** and prioritizing the **"Best Interests[28] of Children and Adolescents"** as the core Vision and Principles.

- **Acknowledging Diversity:** Economies must recognize that legislation concerning minors varies considerably across the region due to political, cultural, and legal differences. Despite this diversity, members should strive to overcome the practical challenges that such differences pose to the global digital ecosystem.
- **Best Interests of the Child:** Children and adolescents are increasingly recognized as independent subjects. At the same time, they are also recognized as individuals who require special protection, particularly given the growing risks they face in the online environment. Accordingly, protecting their rights and safety should be considered in all relevant policy developments.

[28] This expression is widely used, including in *Article 3 of the UN Convention on the Rights of the Child (UNCRC)*

2. Policy Directions

To realize the above vision, member economies should pursue four strategic policy directions to guide their regulatory and practical efforts:

- **Exploring Regulatory Approaches:** Economies should adopt appropriate regulatory measures to protect the privacy of minors. In addition, efforts should be made to enhance interoperability among such regulations, as regulatory fragmentation can pose challenges to compliance and increase legal uncertainty.
- **Enhancing Transparency:** Transparency is fundamental to trust. Policies should focus on ensuring that data processing practices are visible and comprehensible to young users.
- **Securing Technology Neutrality:** Given the rapid pace of digital innovation, regulations should avoid impeding innovation and rigid technical mandates and instead promote flexible, technology-neutral standards to the extent possible given the realities of existing technology and innovation.
- **Guaranteeing “Rights”:** Policies should robustly protect minors as data subjects (e.g., Korean government project to guarantee the “right to be forgotten” of the children and adolescents) while clarifying the role of parents and guardians in exercising these rights.

3. Specific Actionable Tasks

Based on the research findings, APEC members should seek to cooperate on following six concrete tasks to implement the policy directions to the extent permissible by domestic law:

- **Parental Consent**: In many economies, where consent is required for the processing of children’s personal data, consent obtained from a parent or legal guardian is typically required. Economies that have not yet established comparable requirements should consider introducing such provisions.
- **Age-Appropriate Notice:** To bridge the significant gap in transparency, practical measures must be promoted to provide privacy notices in clear, plain language that is easy for children and adolescents to understand. For instance, major tech companies in the Republic of Korea utilize pictures and videos to provide "easy-to-understand privacy policies," and the Philippines' Advisory encourages the use of videos, infographics, and animations to explain privacy terms. Similarly, some platforms in the United States have adopted "privacy dashboards" and teen-focused privacy centers to enhance comprehension.
- **Privacy by Design (PbD):** While legal codification varies, the value of PbD is broadly aligned. APEC should lead continued discussions on practical measures to implement or to encourage implementation of PbD principles effectively across the region. Notable examples include the UK's 'Age Appropriate Design Code (AADC),' which has driven high privacy defaults globally. In the Philippines, the Advisory Guidelines on Child-Oriented Transparency recommend service providers to conduct a Child Privacy Impact Assessment (CPIA) prior to the launch of products or services, thereby integrating child privacy considerations at the design stage. The Republic of Korea also encourages Privacy by Design practices for minors through relevant guidelines. In addition, some corporate initiatives apply privacy protections (e.g., disabling location history) as a default for all children. Some United States

platforms also voluntarily implement “kids mode” and disable targeted advertising for younger users.

- **Effective Age Assurance:** Member economies should explore effective age assurance measures, to the extent possible under member’s domestic law, taking into account risk-proportionate approaches and the principle of data minimization. A practical model could be the layered approach adopted by some major digital service providers, which combines self-declaration, AI-based estimation for general users, and strict verification (e.g., Gov ID) for high-risk services. Additionally, Singapore presents a three-pronged approach using "Age Estimation" (e.g. facial age analysis or voice modeling), "Age Verification" (e.g. Digital ID, passport, driving license), and “Age Inference” (e.g. school enrollment record, financial transaction/possession of a valid credit card, account tenure or activity patterns) as an example of possible approaches.
- **Addressing Profiling and Harmful Content:** As issues like deepfakes and profiling directly impact the dignity and safety of minors, continued policy discussion is warranted to establish safeguards beyond just criminal law frameworks. Leading regulatory examples include Indonesia’s explicit prohibition on profiling children unless it serves their best interests, and the Philippines' Anti-OSAEC Act, which requires ISPs to establish high privacy settings as a default to restrict access to harmful materials. Furthermore, global platforms are voluntarily disabling targeted advertising for users under 13 and requiring opt-in consent for personalized ads for older teens.
- **Education and Awareness**: APEC and member economies must recognize the importance of literacy in empowering data subjects. Continuous and practical efforts—such as education programs and public awareness campaigns targeting both minors and their guardians—are essential to bridge the knowledge gap and ensure that protection mechanisms are effectively utilized. At the same time, efforts should be made to enhance awareness and implementation capacity among businesses.

4. Way Forward and Future Cooperation

To further advance these directions and priorities, APEC and member economies should continue to engage in dialogues and cooperation:

- **Areas for Future Dialogue and Cooperation:** The following topics are particularly complex issues in strengthening data protection for minors and upholding their rights, and therefore merit consideration at the APEC level and beyond:

  - Considering whether and how to broaden who may provide consent on behalf of children (e.g., authorized institutional figures, school principals);
  - Examining protections for older minors who may not fall within the legal definition of a “child” yet remain vulnerable;
  - Considering frameworks to support requests to delete children and adolescent’s personal data as well as mechanisms to support exercising such requests.

- **Harmonization and Information Sharing:** In the execution phase, members should actively share the latest legislative and policy developments. Continuous dialogue is essential to harmonize legal frameworks and bridge the gap between "domestic regulations" and "cross-border services".

Policy Recommendations to Ensure Data Protection and Privacy of Children and Adolescents in Online Space

[Vision and Guiding Principles]

1. **Acknowledging Different Approaches:**
   Economies must recognize that legislation concerning minors varies considerably across the region due to political, cultural, and legal differences. Members should strive to overcome the practical challenges that such differences pose to the global digital ecosystem.

2. **Best Interests of Children and Adolescents:**
   Children and adolescents are increasingly recognized as independent subjects. At the same time, they are also recognized as individuals who require special protection, particularly given the growing risks they face in the online environment. Accordingly, protecting their rights and safety must be the paramount consideration in all policy developments.

[Policy Directions]

3. **Exploring Regulatory Approaches:**
   Economies should adopt appropriate regulatory measures to protect the privacy of minors. In addition, efforts should be made to enhance interoperability among such regulations, as regulatory fragmentation can pose challenges to compliance and increase legal uncertainty.

4. **Enhancing Transparency:**
   Transparency is fundamental to trust. Policies should focus on ensuring that data processing practices are visible and comprehensible to young users.

5. **Securing Technology Neutrality:**
   Given the rapid pace of digital innovation, regulations should avoid rigid technical mandates and instead promote flexible, technology-neutral standards whenever possible.

6. **Guaranteeing "Rights":**
   Policies should robustly protect the rights of minors as data subjects while clarifying the role of parents and guardians in exercising their rights regarding the protection of their children.

[Specific Actionable Tasks]

7. **Parental Consent**:
   In many economies, where consent is required for the processing of children's personal data, consent obtained from a parent or legal guardian is typically required. Economies that have not yet established comparable requirements should consider introducing such provisions.

8. **Age-Appropriate Notice:**
   To bridge the significant gap in transparency, practical measures should be promoted to provide privacy notices in clear, plain language that is easy for children and adolescents to understand.

9. **Privacy by Design (PbD):** While legal codification varies, the value of PbD is broadly aligned. APEC should lead continued discussions on practical measures to implement PbD principles effectively across the region.

10. **Effective Age Assurance:** Member economies should explore effective age assurance measures, taking into account risk-proportionate approaches and the principle of data minimization.

11. **Addressing Profiling and Harmful Content:** As issues like deepfakes and profiling directly impact the dignity and safety of minors, continued policy discussion is warranted to establish safeguards beyond just criminal law frameworks.

12. **Education and Awareness**: Continuous and practical efforts—such as education programs and public awareness campaigns targeting both minors and their guardians—are essential to bridge the knowledge gap and ensure that protection mechanisms are effectively utilized. At the same time, efforts should be made to enhance awareness and implementation capacity among businesses.

[Way Forward and Future Cooperation]

13. **Areas for Future Dialogue and Cooperation:**

- The following topics are particularly complex issues in strengthening data protection for minors and upholding their rights, and therefore merit consideration at the APEC level and beyond:
  - Considering whether and how to broaden who may provide consent on behalf of children (e.g., authorized institutional figures, school principals);
  - Examining protections for older minors who may not fall within the legal definition of a “child” yet remain vulnerable;
  - Considering frameworks to request the deletion of the personal data of children and adolescents as well as mechanisms to support exercising such requests.

14. **Harmonization and Information Sharing:**
    In the execution phase, members should actively share the latest legislative and policy developments. Continuous dialogue is essential to harmonize legal frameworks and bridge the gap between "domestic regulations" and "cross-border services".

Appendix A: Report of the Workshop Result

Workshop Overview

- **Theme:** Ensuring Data Protection and Privacy of Children and Adolescents
- **Date/Venue:** Tuesday, July 29, 2025, 09:30–17:00 / Songdo Convensia (Yeonsu-gu, Incheon)
- **Attendees:**
    - **(Opening Remarks)** Choi Jang-hyuk (Vice Chairperson, Personal Information Protection Commission)
    - **(Welcome Remarks)** Lee Sang-joong (President, Korea Internet & Security Agency)
    - **(Researchers)** Prof. Choi Kyoungjin (Gachon Univ.), Ahn Da-yeon (Yulchon), Han Hye-won (Kim & Chang)
    - **(Speakers)** Marie-Eve Nadeau (Director of International Affairs, 5Rights Foundation), Angela Xu (Senior Privacy Counsel, Google APAC)
    - **(Panelists)** Sarah Inagaki (Policy Advisor, United States Dept of Commerce), Evelyn Goh (Director, International Relations, Policy and Strategy, IMDA Singapore), Claire Todd (Principal Policy Adviser, OPC New Zealand), Mediodecci Lustarini (Secretary General, Komdigi Indonesia), Judith Hannan (Manager, UNICEF EAPRO), Noelle de Guzman (Senior Director, Internet Society)

1. Briefing on Survey and Research Results

(Presenters: Choi Kyoungjin, Ahn Da-yeon, Han Hye-won)

- **(Overview)** A survey and social perception survey were conducted across 21 member economies (11 June – present) to assess the status of child and youth personal data protection policies in the Asia-Pacific region. In-depth analysis was performed through literature review.
- **(Legal Framework)** Member economies primarily regulate child/youth protection through sector-specific laws or within general data protection laws. Only 3 economies have special laws dedicated to child/youth protection.
- **(Parental Consent)** Most members have provisions for parental or legal guardian consent when processing minors' data, though age ranges vary.
    - 13 economies restrict consent authority solely to parents/guardians, while 4 recognize other parties (e.g., school heads).
- **(Notice)** 6 member economies mandate clear and understandable notices specifically for children/adolescents.
- **(Privacy by Design - PbD)** Most members do not mandate PbD specifically for children/adolescents. However, 9 recommend it, and 8 indirectly reflect PbD principles through Privacy Impact Assessments (PIA).

- **(Age Verification)** Most members do not impose a general age verification obligation but enforce substantial obligations through liability provisions or sector-specific laws.
    - Most regulate access to adult/harmful content, with significant variations in verification methods across economies.
- **(Rights)** Most members recognize children/adolescents as data subjects with rights regardless of age, but only 3 explicitly list children/adolescents as separate rights holders.
    - While most recognize a general right to erasure, the United States is unique in specifically regulating a "right to be forgotten" for children/adolescents.
- **(Profiling, etc.)** 4 member economies explicitly prohibit profiling/targeted advertising for children/adolescents; others restrict it indirectly via consent, purpose limitation, or other principles.
- **(Deepfakes & Exploitation)** 2 members explicitly ban deepfakes, while most regulate them indirectly through criminal law, etc.
- **(Self-Regulation)** 8 members support corporate self-regulation efforts through industry codes or limited government support.

2. Lecture: Global Trends and Best Practices in Online Privacy for Children and Adolescents

Talk 1: Marie-Eve Nadeau (5Rights Foundation)

- **(Status & Issues)** Unlike general data, children's personal data includes sensitive and permanent information (identity, emotional state). However, in the digital environment, companies focus on data collection and monetization.
    - Unintentionally provided info (clicks, dwell time, searches) is private, yet children lack control, and this privacy infringement is central to business models.
- **(Approach Direction)** Clear and consistent regulation is needed for innovation to flourish. Innovation must consider all members of society, with respect for children's rights, privacy, and best interests as key elements.
    - Approaches based on consent, notice, and digital literacy have limits; a model where privacy and safety are internalized from the design and default settings is required.
- **(Best Practices)** The UN Convention on the Rights of the Child, offering guidance on applying rights digitally, has evolved into a global commitment and concrete actions.
    - Notably, the UK adopted the 'Age-Appropriate Design Code (AADC)' based on GDPR, driving meaningful changes like age-appropriate design, high privacy defaults, and disabling addictive features.
    - *(Key Content)* Internalizing impact assessments, risk mitigation, and profiling restrictions from the design phase to prevent harm, and strengthening the ICO's enforcement powers.

Talk 2: Angela Xu (Google APAC)

- Google sets 3 core values based on Maslow’s hierarchy of needs to ensure online access while protecting children.
- **(Value 1: Protection)** Applying privacy protection as a default for all children.
    - *(Examples)* Disabling ad personalization and location history, AI-based detection/removal of CSAM, SafeSearch, restricting harmful YouTube ads.
- **(Value 2: Respect)** Respecting diverse parenting styles regarding online access and providing families with choice and flexibility.
    - *(Examples)* 'Family Link' allows supervised account creation, screen time limits, and gradual autonomy based on age.
- **(Value 3: Empowerment)** Strengthening children's information access to support independent exploration and growth.
    - *(Examples)* Google Classroom for education, expert-approved content on Google Play, Google Kids Space.
- **(Age Verification)** Google adopts a layered and proportional approach.
    - Declaration: Input age at account creation (minors switched to supervised accounts).
    - Estimation: Estimate age via search history/usage duration.
    - Verification: Verify age via Gov ID/Credit Card for high-risk services.

Fireside Chat: Choi Kyoungjin, Marie-Eve Nadeau, Angela Xu

- **Q (Choi):** Implications of 5Rights' 'Child & AI Design Code'?
    - **A (5Rights):** The core is to consider privacy and safety as key principles when designing AI for children, giving developers and regulators clear standards on 'what constitutes well-designed AI.'
- **Q (Choi):** How does Google protect children in the AI era?
    - **A (Google):** Priority is ensuring children benefit from AI. Google introduced age-appropriate design and harmful content blocking in ‘Gemini for Teens’ and provides AI education resources.
- **Q (Choi):** With large gaps in laws across APEC, how does Google handle compliance?
    - **A (Google):** Collaborates closely with policy officers for local compliance and uses sandboxes for testing environments. Google also publishes policy papers and legislative frameworks.
- **Q (Choi):** Success factors/challenges for adopting the UK AADC model elsewhere?
    - **A (5Rights):** Harmonization between international cooperation and domestic laws is vital. Since most ratified the UN CRC, forming a common value base is possible.
- **Q (Audience):** How to solve risks of collecting sensitive info for age verification?

    - **A (Google):** Companies also want to minimize collection; often collected due to legal/social demands. Sensitive data is minimized in storage and kept with highest security.
    - **A (5Rights):** Data minimization principles must be observed, and common protection standards are needed to prevent infringement under the guise of collection.

3. Panel Discussion: Challenges and Solutions related to Data Privacy of Children and Adolescents in the Digital Age

(Moderator: Ahn Da-yeon)

- **Indonesia:** Requires guardian consent, but faces challenges like guardian absence, difficulty verifying identity, false info by children, and low parental literacy.
    - *Solutions:* Tiered consent by age, mandatory consent records, verification via Digital ID, parental literacy education, substitute guardian systems.
- **United States:** "Self-declaration" loopholes exist (passing by just entering birthdate). Sophisticated age verification tech is needed based on minimal data collection/disposal.
    - COPPA requires consent only when the operator "actually knows" the user is a child; Epic Games was penalized for avoiding this "knowledge."
- **Singapore:** Age verification is a key gatekeeper but easily bypassed; a comprehensive approach including online safety education is needed.
    - When introducing accurate tools (biometrics, AI), privacy infringement must be considered, and collection minimized.
- **New Zealand:** Principles for age-appropriate design include: 1) Clear purpose, 2) Respect for dignity/welfare, 3) Appropriate permissions (choice/access) by age, 4) Transparency/accountability, 5) Promoting child participation in design.
- **UNICEF:** Expand gov-private cooperation via public funding and regulatory sandboxes to promote child-centric design.
- **ISOC:** Children view privacy as a tool for control and a safety shield. There is concern about "forced consent" for internet use.
    - Reframe concepts (e.g., "Cookies" -> "Data Collectors") to fit children's level. Shift to transparent, user-centric data processing.
- **Indonesia (Accountability):** Appoint DPOs, conduct PIAs, introduce/encourage Child Privacy Certification.
    - *Transparency:* 1) Clear/concise notice (visuals), 2) Records of processing, 3) Ban on nudges/manipulative practices, 4) Explanation/objection mechanisms for algo-profiling, 5) Encourage 3rd party audits.
- **UNICEF:** Sustain child participation throughout the product lifecycle (design, dev, operation).
- **United States:** Provide tools to manage/delete digital footprints to both children and parents.

    - Parallel efforts to raise awareness (FTC's 'You Fill' program). International cooperation needed as laws like the 'Take It Down Act' apply only to Americans.
- **Singapore:** Guardian consent may not always represent the child's best interest. Periodic consent reviews and modification/withdrawal tools are needed. Support parents to communicate with children and use services responsibly.
- **New Zealand:** Education on rights and how to exercise them is needed for kids and parents. Regulators should distribute practical, plain-language guidelines by sector and visit the field for explanation/feedback.
- **ISOC:** Technical community role is crucial for developing standards/protocols like auto-safety modes or encryption.

4. Small Group Discussion: Developing Policy Recommendations with Actionable Guidelines

- **Group 1: Parental Consent** (Korea; Papua New Guinea; Chinese Taipei; United States)
    - Consensus that guardian consent is necessary for processing minor's data.
    - Expanding "guardian" scope (to school heads, etc.) has merit but requires caution regarding infringement of parental rights.
- **Group 2: Child-Friendly Notice** (Korea; Mexico; the Philippines; Chinese Taipei; and UNICEF)
    - Broad consensus on implementing mechanisms to confirm children/adolescents *actually read and understood* the notice.
    - However, age ranges for applying these notices vary by economy.
- **Group 3: Age Verification** (ISOC; Korea; Singapore; and Chinese Taipei)
    - Agreed that effective verification is needed but *verifying* it is extremely difficult.
    - Need concrete discussions based on case studies. Proportional verification based on regulatory need/protection level is required, combined with self-regulation/PbD.
    - AI can be used, but must balance with data minimization principles.
- **Group 4: Support for Exercising Rights** (Indonesia; Korea; the Philippines; United States)
    - Whether specific rights (e.g., right to be forgotten) are specified varies greatly by economy.
    - Agreed that "Awareness" is key, requiring differentiated education based on developmental stages.
- **Group 5: Targeted Ads & Online Sexual Exploitation** (Indonesia; Korea; New Zealand; Papua New Guinea; the Philippines)

    - General consensus on the need for legal requirements to prevent harm, emphasizing a proportional approach based on risk/harm rather than a uniform one.
    - Considerations: Gov admin burden, corporate compliance costs, reasonable transition periods.
    - Self-regulation is important but cannot be the primary tool due to conflicts of interest.
- **Group 6: Age-Appropriate Design** (5Rights; Korea; Singapore; and Viet Nam)
    - Agreed on the need for a regulatory model requiring age-appropriate design. Government role: 1) Establish common principles via guidelines/codes, 2) Provide clarity, 3) Promote self-regulation.
    - Comprehensive regulation is hard; sharing best practices (PbD) is key.
    - PbD should include risk assessment, age verification, disabling location tracking, clear notice. PETs (Privacy Enhancing Technologies) need layered application to address re-identification risks.

5. Closing: Key Outcomes and The Way Forward

(Presenter: Director Choi Yoon-jung)

1. **(Recognizing Diversity)** Legal systems vary greatly, posing real challenges. Children are increasingly recognized as independent subjects, but protection needs are also growing.
2. **(Need for Regulatory Clarity)** Disparate laws make compliance difficult. Interest is growing in enhancing cross-border dialogue and seeking common principles.
3. **(Improving Notice Transparency)** A large gap exists in age-appropriate notices. Promote practical means for clear, plain-language notices to enhance transparency.
4. **(Common Understanding of PbD)** Few define PbD in law, but broad consensus exists on its value. Continued discussion on practical support tools is needed.
5. **(Consistency in Age Verification)** Most lack general obligations; application varies by sector. Need to explore tech-neutral, interoperable methods.
6. **(Clarifying Roles and Rights)** Rights (e.g., to be forgotten) are widely recognized. However, the role relationship with parents needs definition and deep regional discussion.
7. **(Profiling & Harmful Content)** Clear regulation on profiling is rare; harmful content is mostly criminal law. Legal bases for takedowns vary. Policy discussions must continue.
8. **(Future Areas for Dialogue)** Continued discussion needed on: 1) Separate legal bases for processing (incl. guardian consent), 2) Expanding guardian scope, 3) Protection for adolescents (post-childhood), 4) Verifiable consent mechanisms, 5) Bundled consent practices.

9. **(Reaffirming Joint Commitment)** Overwhelming consensus exists on protecting children's digital rights. Stakeholders must strive for common understanding and global frameworks through ongoing discussion.

6. Implications

- **(Domestic Policy)** Reference overseas cases when establishing domestic policies currently underway, such as expanding protection targets, differentiating protection by age group, legislating the digital right to be forgotten, and improving the legal representative consent system.
- **(International Cooperation)** While child/youth privacy is discussed in major economies, discussions in the Asia-Pacific need further progress. Use this APEC project to expand regional discussions and demonstrate Korea's global leadership.

Appendix B: Social Perception Survey

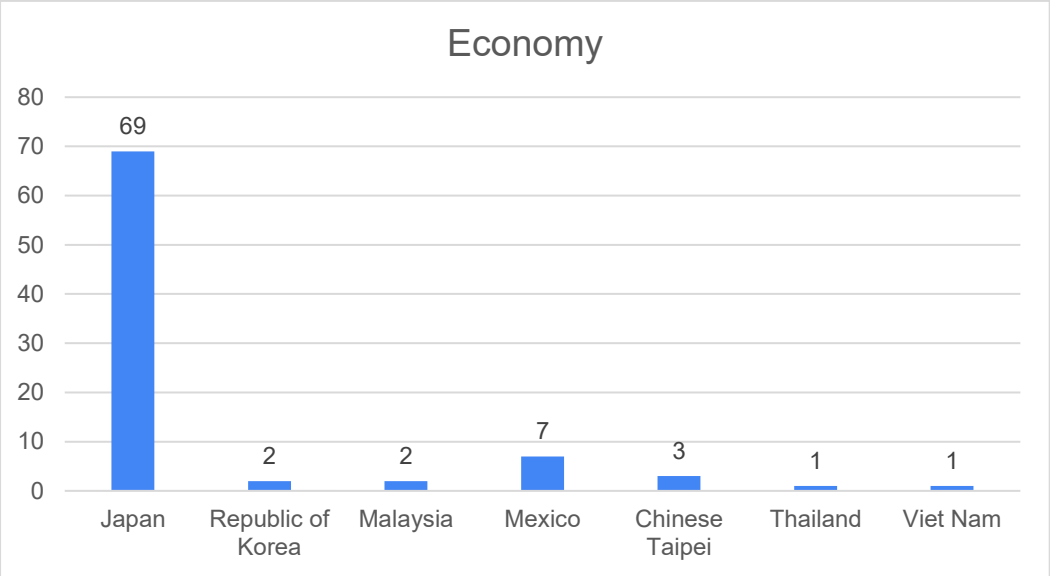
I. Introduction

As part of this APEC research project, a social perception survey was conducted to assess how the general public across APEC member economies perceive the personal data and privacy protection of children and adolescents. The purpose of this survey is to compare and analyze public awareness levels among economies and to identify factors that may inform efforts to strengthen child and youth privacy protection in the APEC region moving forward. The responses collected are used solely for statistical and analytical purposes, and the aggregated results may be shared with governments and organizations of APEC member economies, relevant public institutions, and the broader public to support evidence-based policy development.

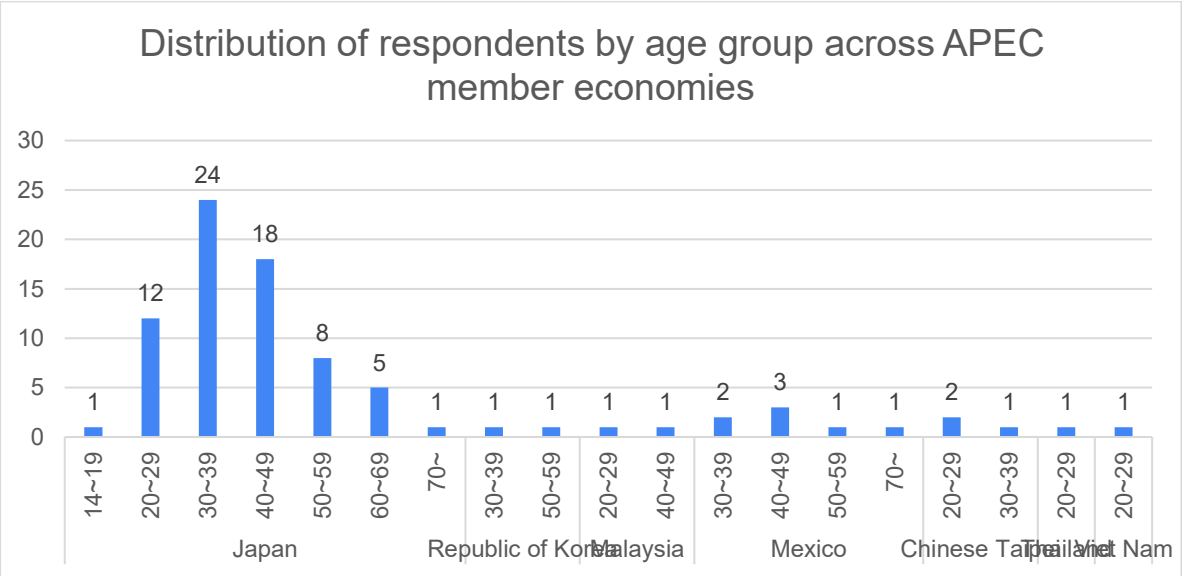
Despite efforts to administer the survey across all 21 APEC member economies, there were practical challenges in publicizing and distributing the survey through APEC focal points, which resulted in an insufficient number of respondents overall (85 respondents from seven member economies) and an overrepresentation of responses from certain economies (i.e. 69 respondents from Japan). These limitations mean that the findings cannot be interpreted as a fully representative assessment of the general public's perceptions across the entire APEC region. Nevertheless, the survey provides the most recent cross-economy snapshot of public awareness regarding the personal data and privacy protection of children and adolescents, and it is expected to serve as a meaningful foundational resource for future APEC policy development in this area.

II. Demographic analysis

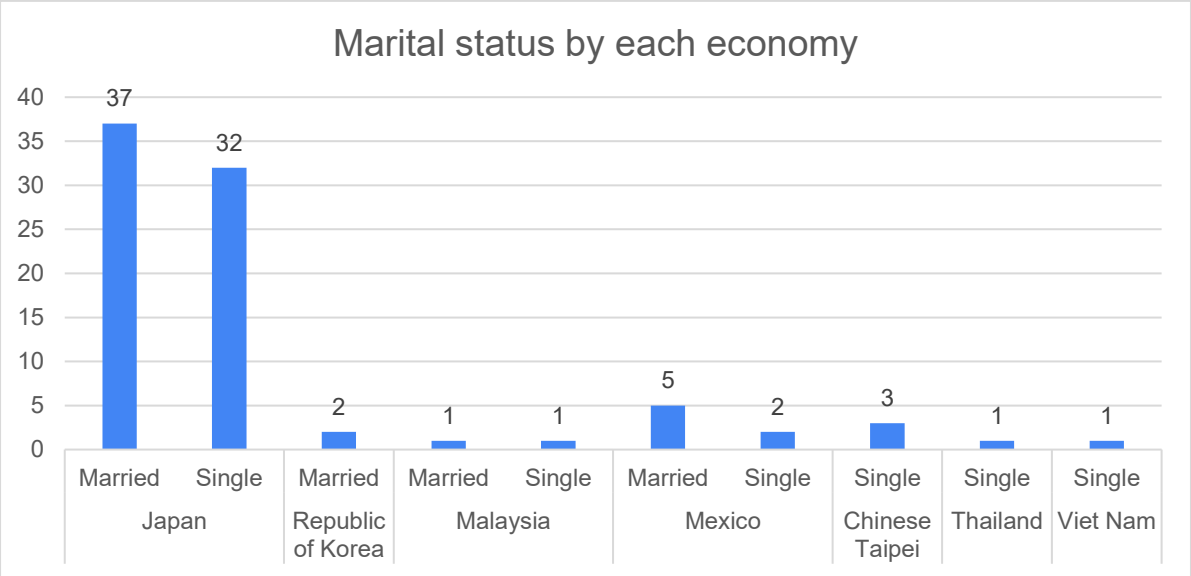
The social perception survey collected responses from seven APEC member economies, but the distribution of participants was highly uneven across economies. A substantial majority of responses came from Japan (69 respondents, approximately 86%), while only a small number were received from Korea (2 respondents); Malaysia (2); Mexico (7); Chinese Taipei (3); Thailand (1); and Viet Nam (1). This skewed distribution reflects the challenges encountered during survey dissemination and means that the demographic profile is disproportionately influenced by Japanese respondents.

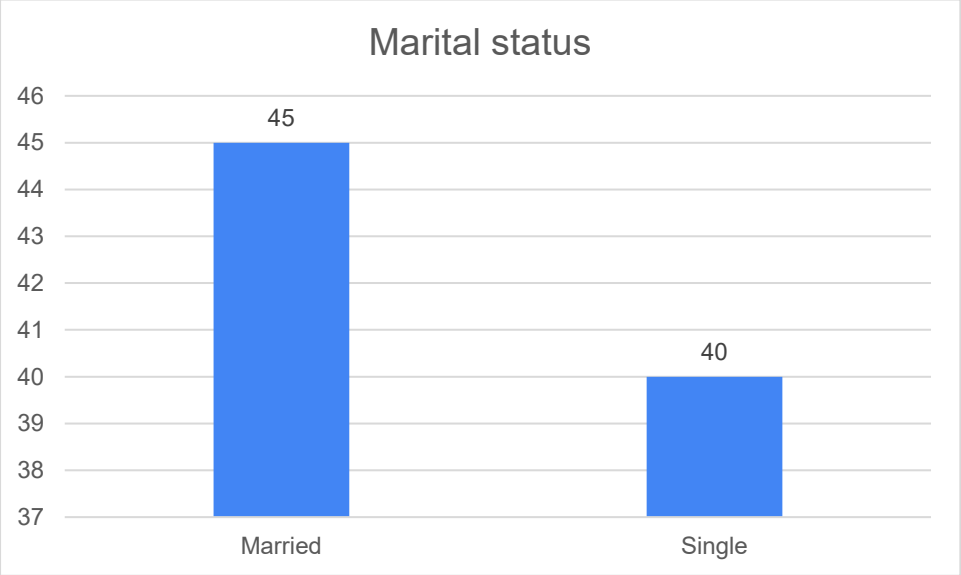


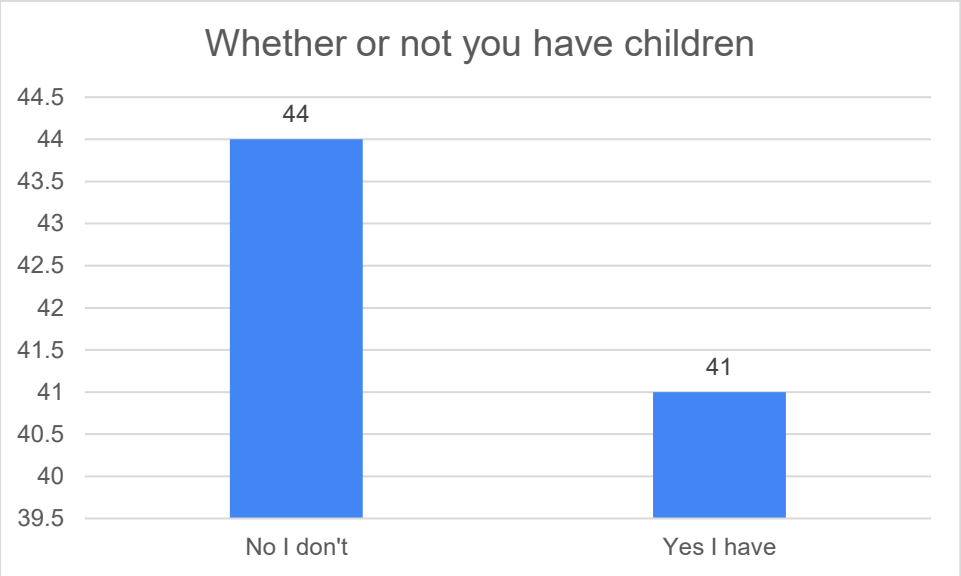
Across all economies, the age distribution shows a concentration in the 30–39 age group (28 respondents, 35%), followed by 40–49 (22 respondents, 28%), and 20–29 (17 respondents, 21%). Smaller proportions were represented in the 50–59 age bracket (10 respondents) and older groups, such as 60–69 (5 respondents) and 70+ (2 respondents). Only one respondent fell within the 14–19 adolescent age category, indicating that the survey primarily reflects adult perspectives rather than youth viewpoints.



In terms of marital status, respondents were relatively balanced between those who are married (45 respondents, 53%) and those who are single (40 respondents, 47%), suggesting no major demographic skew in family status. Responses were also evenly distributed regarding parental status: 44 respondents (52%) indicated that they do not have children, while 41 respondents (48%) reported having children. This near-even split allows for some comparison of attitudes between parents and non-parents, although the small sample size outside Japan limits economy-specific interpretation.


Marital status by each economy
40
35
30
25
20
15
10
5
0
37
32
2
1
1
5
2
3
1
1
Married
Single
Married
Married
Single
Married
Single
Single
Single
Single
Japan
Republic of Korea
Malaysia
Mexico
Chinese Taipei
Thailand
Viet Nam

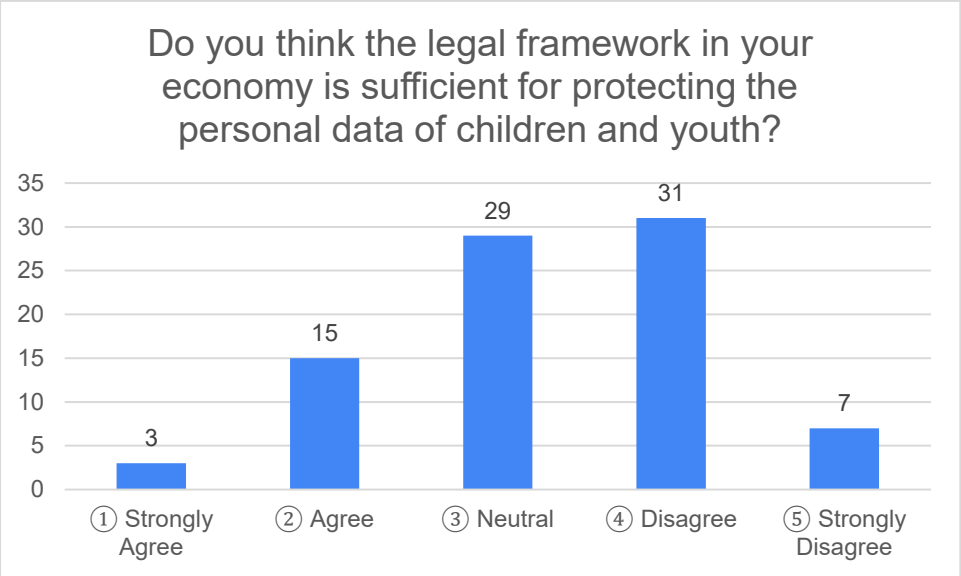

Marital status
46
45
44
43
42
41
40
39
38
37
45
40
Married
Single



Overall, the demographic characteristics of the survey responses are heavily shaped by the overwhelming participation from Japan and the limited number of respondents from other economies. While the dataset provides useful qualitative insights, the demographic imbalance suggests caution in generalizing the findings to the broader APEC population.

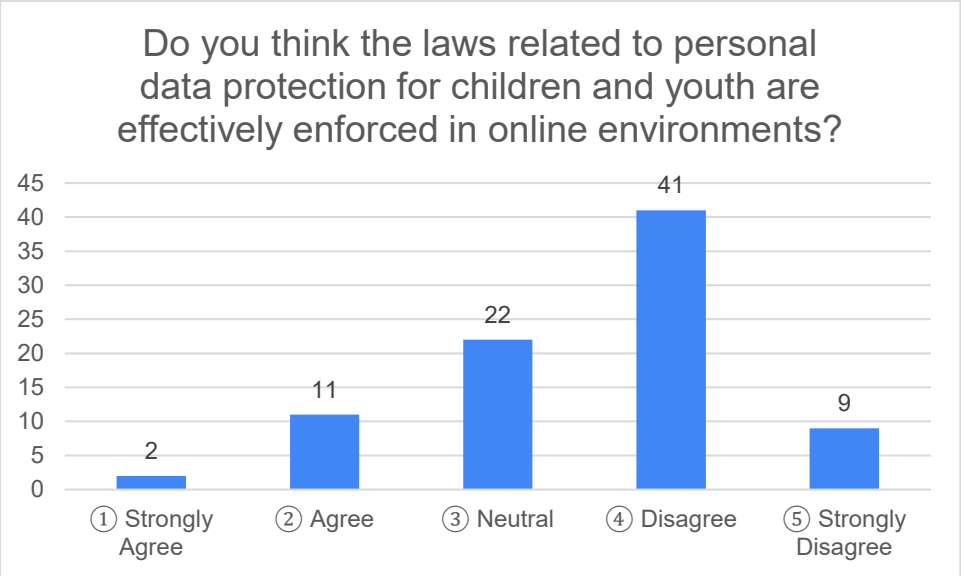
III. Do you think the legal framework in your economy is sufficient for protecting the personal data of children and youth?

Responses to the question about whether the legal framework in each economy is sufficient to protect the personal data of children and youth show a generally critical or uncertain public perception. A plurality of respondents answered “Disagree” (31 respondents), indicating that many believe their current legal framework is not adequate. This is closely followed by “Neutral” (29 respondents), suggesting substantial uncertainty or lack of awareness regarding the legal protections in place. Only 15 respondents selected “Agree”, and very few expressed strong positive sentiment, with just 3 respondents choosing “Strongly Agree.” In contrast, 7 respondents chose “Strongly Disagree,” reflecting a minority with strongly negative views. Overall, these results suggest that public confidence in the sufficiency of existing legal frameworks for protecting children's and adolescents’ personal data is relatively low, with many respondents either doubtful of their adequacy or unsure about the level of protection currently provided.



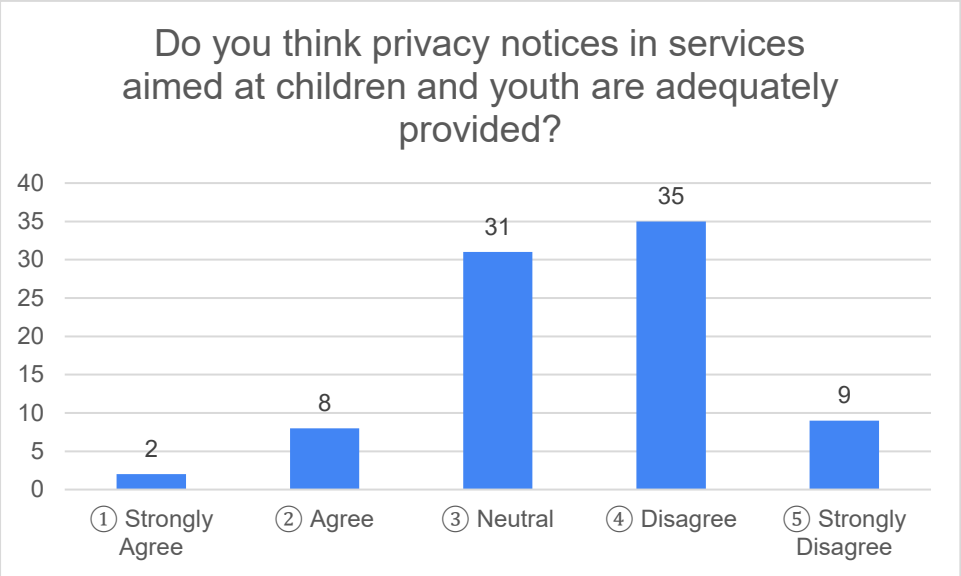
IV. Do you think the laws related to personal data protection for children and youth are effectively enforced in online environments?

Responses to this question indicate a broadly skeptical view of how effectively personal data protection laws for children and youth are enforced in online environments. The most common answer was “Disagree” (41 respondents), suggesting that a significant portion of participants believe enforcement is insufficient. This is followed by “Neutral” (22 respondents), reflecting considerable uncertainty or lack of visibility into how enforcement actually operates. Only 11 respondents indicated “Agree,” while positive confidence remained very low, with just 2 respondents selecting “Strongly Agree.” Additionally, 9 respondents chose “Strongly Disagree,” reinforcing the perception that enforcement mechanisms are weak or ineffective. Overall, the results suggest that public confidence in the online enforcement of child and youth data protection laws is limited, with the majority of respondents either doubtful of enforcement effectiveness or unsure whether meaningful enforcement is taking place.



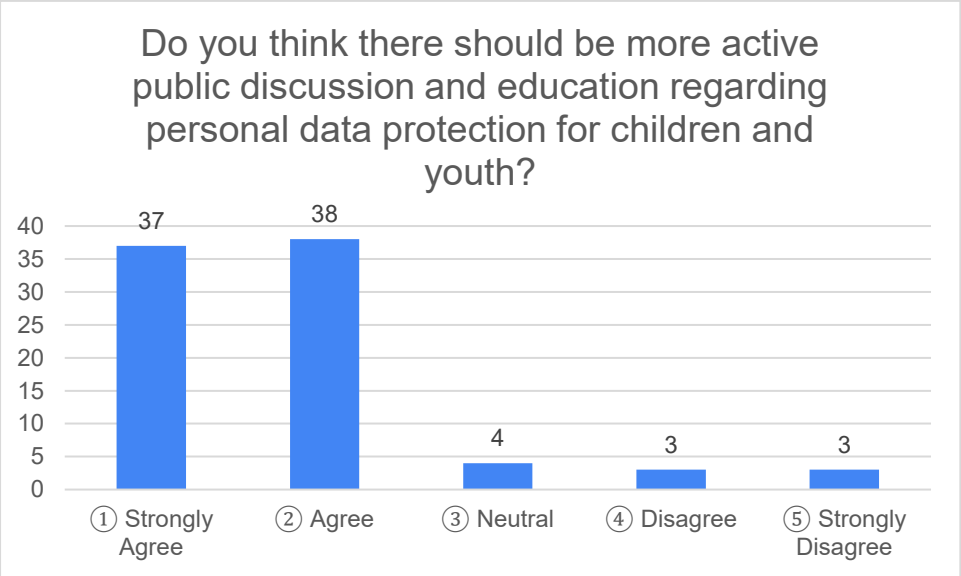
V. Do you think privacy notices in services aimed at children and youth are adequately provided?

Survey responses reveal a predominantly critical view regarding the adequacy of privacy notices in services directed toward children and youth. The largest share of respondents selected “Disagree” (35 respondents), indicating that many believe such services do not provide sufficiently clear, accessible, or age-appropriate privacy notices. This was followed closely by “Neutral” (31 respondents), suggesting considerable uncertainty or lack of awareness about whether current notices meet required standards. More strongly negative sentiment is reflected in the 9 respondents who chose “Strongly Disagree.” Positive perceptions were comparatively rare: only 8 respondents agreed that privacy notices are adequately provided, and just 2 respondents expressed strong agreement. Overall, the results indicate low public confidence in the adequacy of privacy notices for children and youth, with most respondents either dissatisfied or unsure about the level of transparency and child-appropriate communication provided by online services.



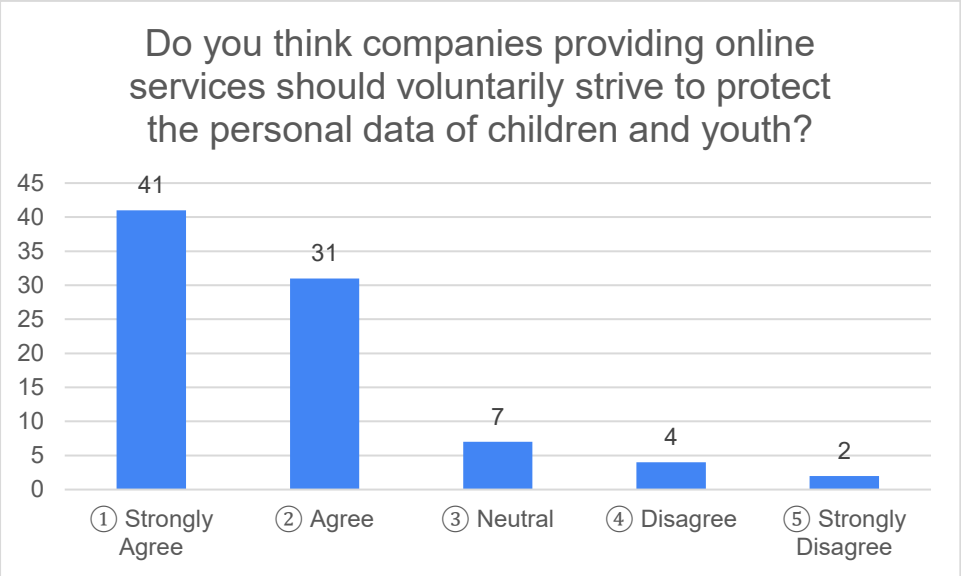
VI. Do you think there should be more active public discussion and education regarding personal data protection for children and youth?

Responses to this question show overwhelming support for expanding public discussion and education on personal data protection for children and youth. The majority of participants expressed a clearly positive view, with 38 respondents selecting “Agree” and 37 respondents choosing “Strongly Agree.” Together, these groups account for 75 out of all respondents, indicating a broad consensus that greater public engagement and awareness-raising efforts are needed. Only a small number of respondents were uncertain, with 4 selecting “Neutral,” while negative views were very limited: 3 respondents chose “Disagree,” and another 3 selected “Strongly Disagree.” Overall, the findings demonstrate a strong regional desire for more active public dialogue, education, and outreach initiatives to strengthen understanding and protection of children’s and adolescents’ personal data.



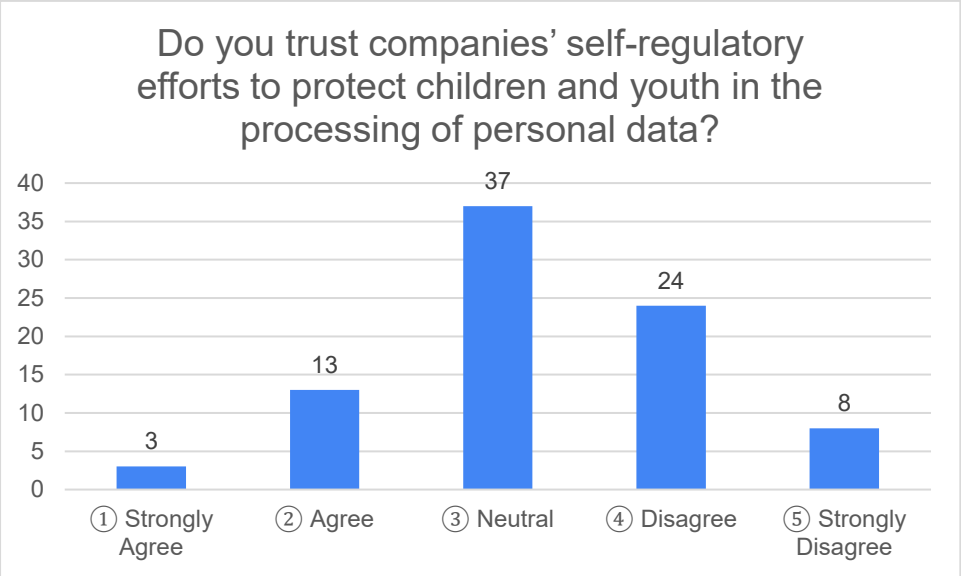
VII. Do you think companies providing online services should voluntarily strive to protect the personal data of children and youth?

Survey respondents expressed very strong support for the idea that companies providing online services should voluntarily take greater responsibility in protecting the personal data of children and youth. The largest group of participants selected “Strongly Agree” (41 respondents), and another 31 respondents chose “Agree,” indicating that more than 90% of all respondents believe companies should adopt proactive and voluntary safeguards beyond legal requirements. Only a small minority expressed neutrality (7 respondents) or disagreement (4 respondents selecting “Disagree” and 2 selecting “Strongly Disagree”). These results suggest that the public places significant expectations on online service providers to implement child-centered privacy protections, reflecting a widespread belief that industry should play an active and responsible role in safeguarding minors’ personal data in the digital environment.



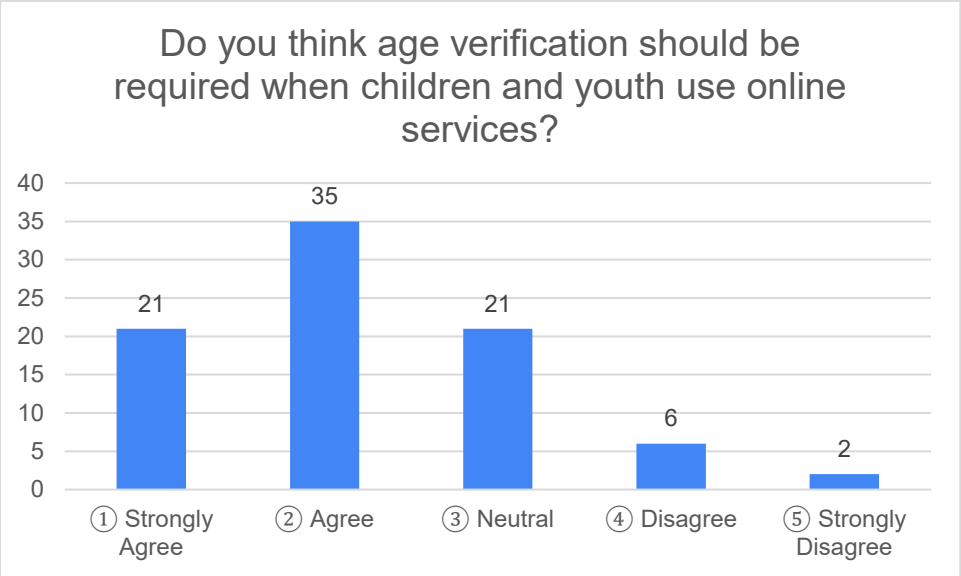
VIII. Do you trust companies' self-regulatory efforts to protect children and youth in the processing of personal data?

The responses this question indicate a generally low level of trust in companies' self-regulatory efforts to protect children and youth when processing personal data. The most common response was "Neutral" (37 respondents), suggesting that many participants are uncertain or lack sufficient information to evaluate the effectiveness of corporate self-regulation. However, among those who expressed a clear opinion, negative views outweighed positive ones: 24 respondents selected "Disagree" and 8 selected "Strongly Disagree," indicating substantial skepticism toward voluntary corporate measures. In contrast, positive perspectives were limited, with only 13 respondents choosing "Agree" and 3 respondents selecting "Strongly Agree." Overall, the results suggest that the public does not place strong confidence in companies' voluntary efforts and expects more robust oversight, accountability, or legal requirements to ensure adequate protection of children's and adolescents' personal data.



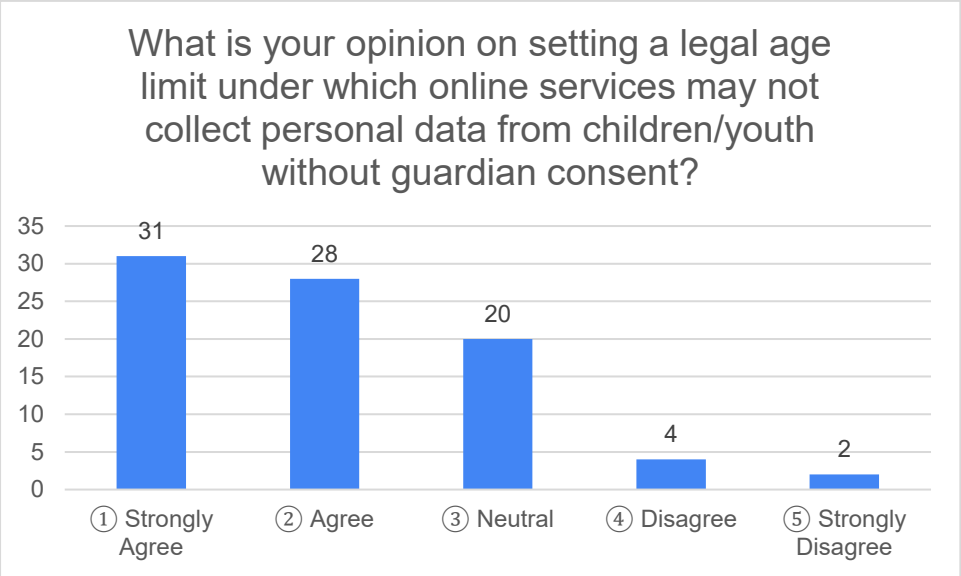
IX. Do you think age verification should be required when children and youth use online services?

Survey respondents expressed generally strong support for requiring age verification when children and youth use online services. The majority selected positive responses, with 35 respondents choosing “Agree” and an additional 21 selecting “Strongly Agree.” Together, these groups represent more than 70% of all participants, indicating broad public recognition of age verification as an important safeguard for minors online. Although 21 respondents selected “Neutral,” suggesting some uncertainty or ambivalence about how such systems should operate in practice, only a small minority expressed opposition, with 6 respondents choosing “Disagree” and 2 selecting “Strongly Disagree.” Overall, the data reveals a clear consensus that age verification is viewed as a necessary protective measure for children and adolescents in digital environments.



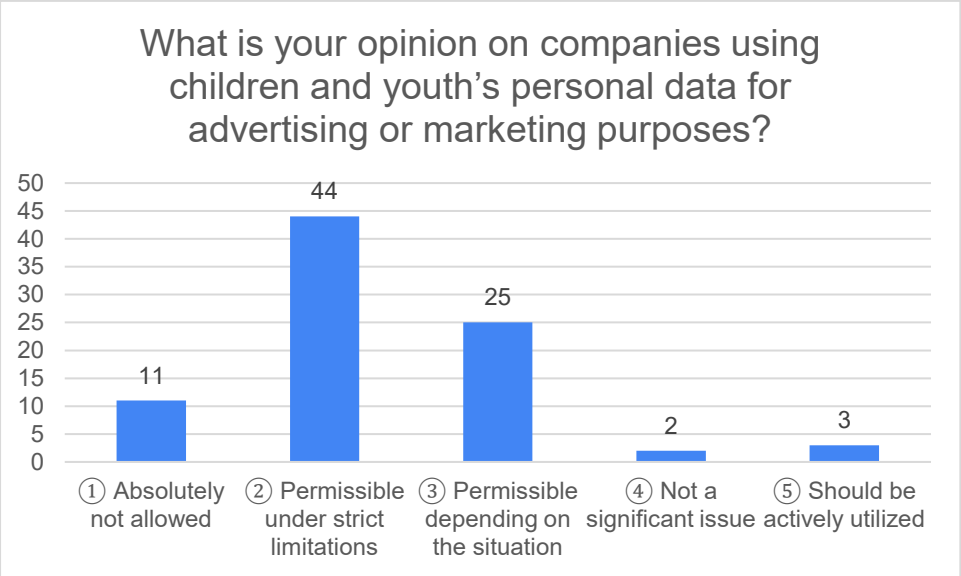
X. What is your opinion on setting a legal age limit under which online services may not collect personal data from children/youth without guardian consent?

The responses show strong public support for establishing a legal age threshold below which online services are prohibited from collecting personal data without guardian consent. A significant portion of participants expressed positive views, with 31 respondents selecting “Strongly Agree” and 28 choosing “Agree.” Together, these account for nearly three-quarters of all respondents, indicating broad consensus on the need for a clear legal safeguard tied to age. While 20 respondents selected “Neutral,” reflecting some uncertainty about how such a threshold should be determined or implemented, opposition was minimal: only 4 respondents chose “Disagree,” and 2 selected “Strongly Disagree.” Overall, the findings demonstrate a high level of public endorsement for legally mandating guardian consent for younger users, underscoring strong societal expectations for structured and enforceable protections for children’s and adolescents’ personal data.



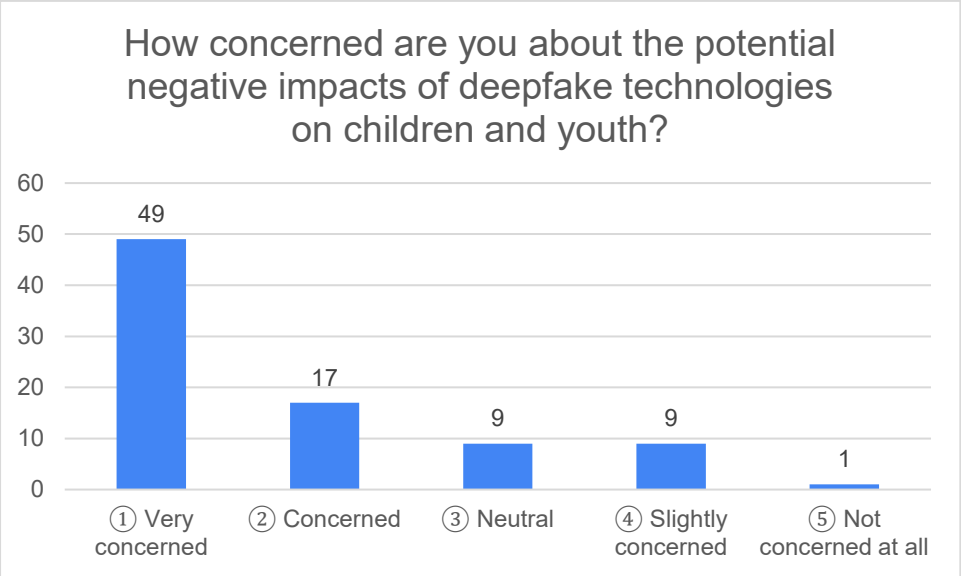
XI. What is your opinion on companies using children and youth's personal data for advertising or marketing purposes?

Respondents expressed generally cautious and restrictive attitudes toward the use of children's and adolescents' personal data for advertising or marketing purposes. The most common view was "Permissible under strict limitations" (44 respondents), indicating that many participants accept such practices only if strong safeguards and regulatory controls are in place. Another 25 respondents chose "Permissible depending on the situation," suggesting a more conditional acceptance that varies based on context, purpose, or levels of risk. Notably, a substantial minority—11 respondents—selected "Absolutely not allowed," reflecting strong opposition to any marketing use of minors' data. Only a small number viewed the issue more permissively: 3 respondents believed such data "should be actively utilized," and 2 respondents considered it "not a significant issue." Overall, the results reveal a clear trend toward caution, with the majority favoring strict limits or careful case-by-case evaluation, and relatively few endorsing broad or unrestricted commercial use of children's and adolescents' personal data.



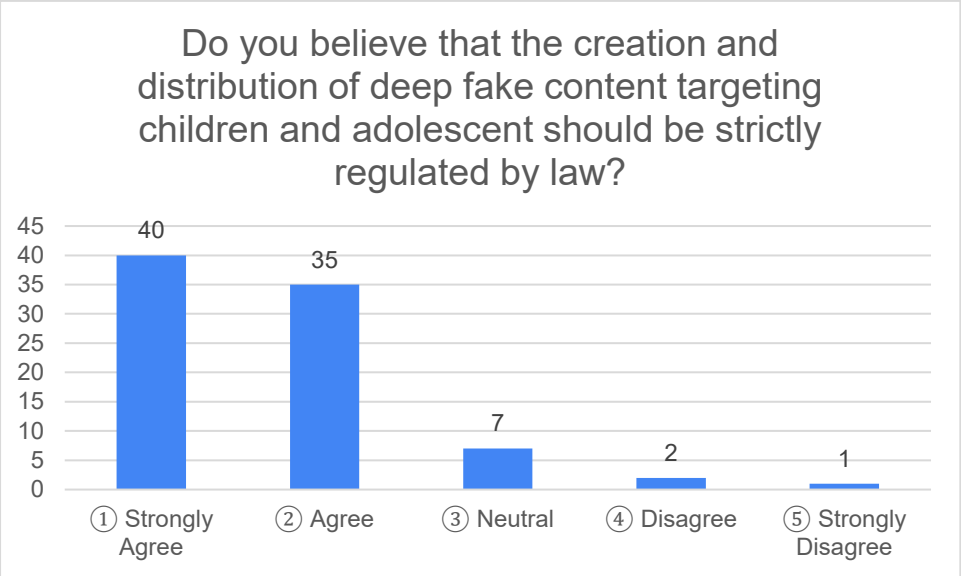
XII. How concerned are you about the potential negative impacts of deepfake technologies on children and youth?

Survey participants expressed high levels of concern about the potential negative impacts of deepfake technologies on children and youth. The majority selected strongly worried responses, with 49 respondents choosing “Very concerned” and 17 selecting “Concerned.” Together, these account for a clear supermajority, indicating widespread recognition of deepfakes as a serious emerging threat to minors. A smaller number of respondents—9 choosing “Neutral” and 9 choosing “Slightly concerned”—expressed more moderate or uncertain views, suggesting that some individuals may lack awareness of the risks or feel unsure about the severity of the threat. Only one respondent selected “Not concerned at all,” representing negligible outright dismissal of the issue. Overall, the results underscore a strong public perception that deepfake technologies pose substantial and pressing risks to the safety, privacy, and psychological well-being of children and adolescents.



XIII. Do you believe that the creation and distribution of deep fake content targeting children and adolescent should be strictly regulated by law?

The survey results show overwhelming public support for strict legal regulation of deepfake content targeting children and adolescents. A large majority of participants selected positive responses, with 40 respondents choosing “Strongly Agree” and 35 choosing “Agree.” Together, these account for nearly all respondents, reflecting a clear consensus that deepfake content involving minors should be subject to stringent legal controls. Only a small number of participants expressed uncertainty, with 7 respondents selecting “Neutral.” Opposition was extremely limited: just 2 respondents chose “Disagree,” and 1 selected “Strongly Disagree.” Overall, the data demonstrates strong public demand for robust legal intervention to prevent the creation and distribution of deepfake content targeting children and adolescents, underscoring widespread concern about the severe risks such technologies pose to minors.



XIV. What do you think is the most important factor to consider for future personal data protection of children and youth? (Optional: Please feel free to elaborate below.)

Although this was an optional open-ended question, a diverse range of respondents provided meaningful insights on the factors they believe are most important for the future protection of children's and adolescents' personal data. Several key themes emerged. Many respondents emphasized the legal and regulatory framework, calling for stronger laws, clearer rules, and more standardized regulations to protect minors online. Others highlighted the importance of education, noting that both children and parents require better digital literacy, awareness of risks, and guidance on safe online behavior.

A number of respondents stressed the need to center children's rights and participation, arguing that minors should be empowered to understand and exercise control over their personal data, including consent and self-determination. Several comments focused on privacy and safety, including the need to prevent misuse of data, address crimes such as fraud or exploitation, and ensure that children can hide or withdraw information when necessary.

There were also responses advocating for stronger corporate responsibility and self-regulation, suggesting that platform providers must adopt more protective policies and stricter internal safeguards. In addition, some participants pointed to the challenges posed by children using multiple international apps and platforms, underscoring the need for cross-border alignment and consistent standards.

Taken together, the responses reveal broad public recognition that future child and youth data protection requires a combination of strong laws, effective education, child-centered rights protections, responsible industry practices, and holistic digital safety measures.