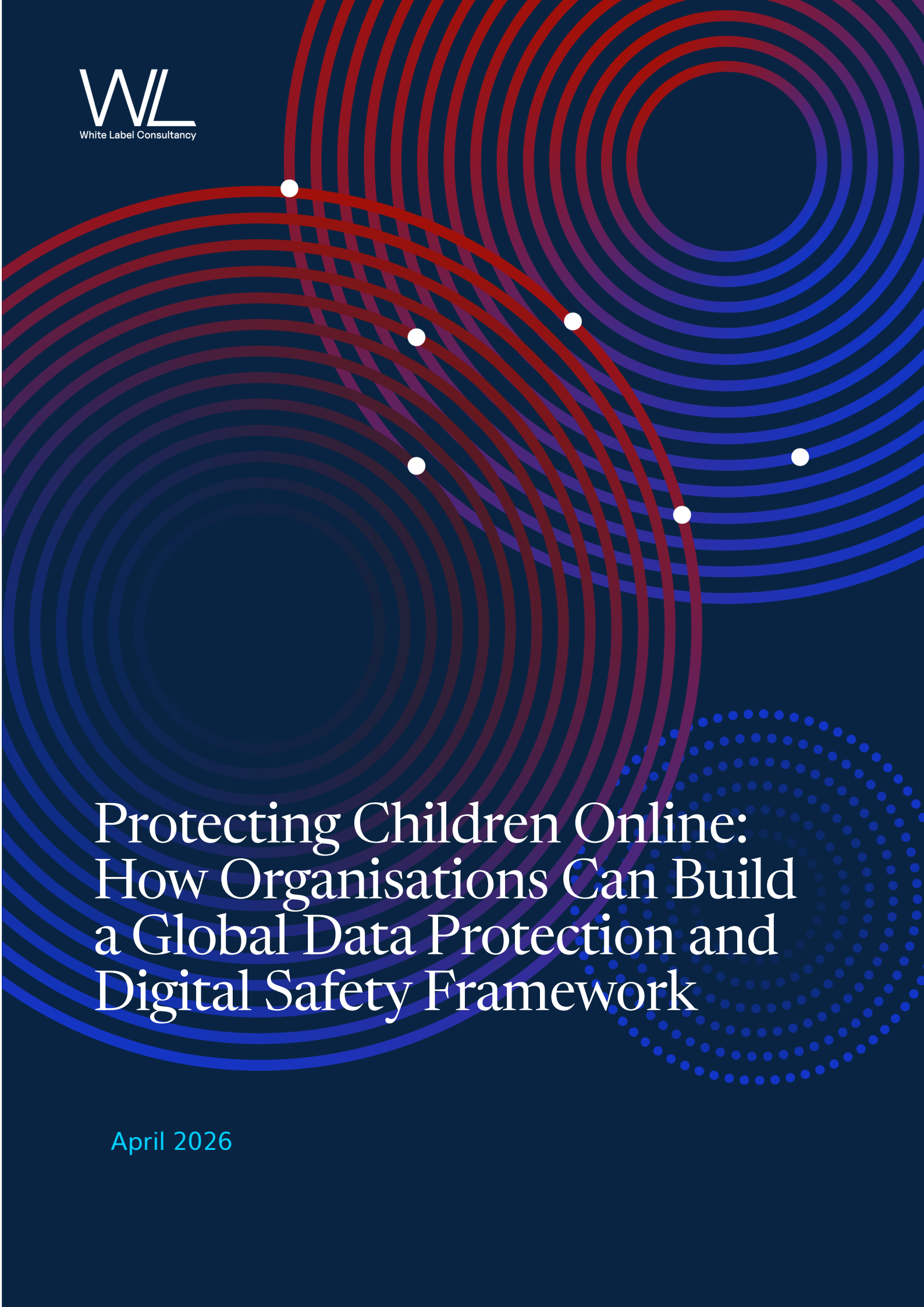




Protecting Children Online: How Organisations Can Build a Global Data Protection and Digital Safety Framework

April 2026

Table of Contents

1. Introduction.....	4
2. Children in Digital Environments: Structural Vulnerabilities and Key Risks.....	4
<i>Behavioural Profiling and Targeted Advertising</i>	<i>5</i>
<i>Manipulative Design and Engagement-Driven Systems</i>	<i>6</i>
<i>Lack of Transparency and Meaningful Consent.....</i>	<i>6</i>
<i>AI-Driven Systems and Emerging Risks.....</i>	<i>6</i>
3. The Global Regulatory Landscape	7
<i>European Union and United Kingdom</i>	<i>11</i>
<i>United States and Canada</i>	<i>11</i>
<i>Latin America</i>	<i>12</i>
<i>GCC and Middle East.....</i>	<i>12</i>
<i>Asia-Pacific</i>	<i>13</i>
4. What Regulators Expect: Core Compliance Mechanisms.....	14
<i>Parental Consent and Age Assurance</i>	<i>14</i>
<i>Restrictions on Profiling and Targeted Advertising</i>	<i>14</i>
<i>Privacy-by-Design and Age-Appropriate Design.....</i>	<i>15</i>
<i>Transparency Adapted to Children</i>	<i>15</i>
<i>Risk-Based Governance and Impact Assessments</i>	<i>15</i>
<i>The Overall Direction of Travel</i>	<i>16</i>
5. Cross-Border Compliance Challenges	16
6. Practical Compliance Framework for Organisations	17
<i>Assess Whether Services Are Likely to Be Accessed by Children</i>	<i>17</i>
<i>Map Children's Data Processing Activities</i>	<i>18</i>
<i>Conduct Child-Specific Data Protection Impact Assessments</i>	<i>18</i>
<i>Implement Age-Appropriate Design Principles</i>	<i>18</i>

<i>Review Advertising, Profiling, and Algorithmic Systems</i>	<i>18</i>
<i>Strengthen Governance Structures and Internal Accountability</i>	<i>19</i>
<i>Provide Transparency and Parental Control Tools</i>	<i>19</i>
7. Strategic Opportunities - From Reactive Compliance to Safer Product Design	19
<i>Compliance as a Product and Design Function</i>	<i>19</i>
<i>Trust as a Competitive Differentiator</i>	<i>20</i>
<i>Global Standardisation as Operational Simplification.....</i>	<i>20</i>
<i>Governance Synergies Across Risk Domains</i>	<i>20</i>
<i>Preparedness for the Next Regulatory Wave.....</i>	<i>21</i>
8. Conclusion - Navigating Children’s Data Protection and Digital Safety Globally.....	21

Abstract

The processing of children's personal data has become one of the most closely scrutinised areas of global digital regulation. As minors engage with social media, gaming platforms, educational technologies, and AI-driven services from an increasingly early age, regulators across jurisdictions are moving beyond traditional consent-based models toward structural obligations covering how digital services are designed, governed, and operated. Regulatory expectations are converging around five core principles: privacy-by-design and privacy-by-default safeguards; age-appropriate design requirements; restrictions on behavioural profiling and targeted advertising; enhanced transparency obligations; and risk-based governance measures including data protection impact assessments. This paper examines the principal privacy and digital safety risks associated with children's data processing, analyses the evolving regulatory landscape across major jurisdictions in Europe, North America, Latin America, the Middle East, and Asia-Pacific, identifies the cross-border compliance challenges organisations face, and sets out a practical framework for embedding child-centric safeguards into governance structures, product design, and operational controls.

1. Introduction

Children participate in digital environments from an early age through social media, gaming platforms, educational applications, connected devices, and AI-driven services.¹

They are, however, less likely than adults to understand how their data is collected, analysed, or retained, or to appreciate the long-term consequences of profiling and behavioural targeting which leads to an asymmetry between the sophistication of data-driven systems and the capacity of younger users to understand or resist them.

Against this backdrop, this paper examines the evolving global framework governing children's personal data and digital safety. It identifies the principal risks affecting children in digital environments, reviews key regulatory developments across major jurisdictions, and analyses the cross-border compliance

challenges these create for organisations operating internationally. It concludes with a practical framework to help organisations translate emerging legal expectations into governance structures, product design decisions, and operational controls.

2. Children in Digital Environments: Structural Vulnerabilities and Key Risks

Three structural factors underpin regulator's concerns about children in digital environments.

The 1st is the scale and persistence of data collection. Children's interactions with online services generate detailed and continuous streams of behavioural data - aggregated, analysed, and retained over long periods in ways that most younger users neither observe nor understand. These data contribute to

¹ OECD (2025), *How's Life for Children in the Digital Age?*, OECD Publishing, Paris, <https://doi.org/10.1787/0854b900-en>.

digital profiles that can influence future opportunities, access to services, and reputational outcomes well into adulthood. The potential for lasting consequences arising from data generated during childhood has led regulators to treat early-stage data collection as particularly sensitive, and to question whether any consent mechanism, however well designed, is adequate to address risks of this nature and duration.

The 2nd is the developmental reality of childhood itself. The cognitive and emotional development of minors leaves them structurally less equipped to recognise data collection practices, evaluate the implications of consent, or resist design features engineered to influence behaviour.² This is not a gap that better information or clearer notices can close - it is a condition that regulators increasingly treat as requiring intervention at the level of the service itself, not at the level of the individual user.

The 3rd is the structural misalignment between data-driven business models and children's interests. Platforms designed to maximise engagement, personalise content, and monetise behavioural data operate according to a logic that is indifferent to the age or vulnerability of the user generating that data.³ When applied to children, this misalignment produces a set of concrete and well-documented risks.

Behavioural Profiling and Targeted Advertising

Children's online activities may reveal detailed information about their habits, interests, social interactions, and emotional states - data points that can be aggregated into profiles capable of predicting behaviour and influencing engagement. Unlike contextual advertising, which is linked to the content being viewed, behavioural advertising operates by tracking users across services and over time, allowing advertisers to tailor messages in ways that may exploit children's limited ability to critically assess persuasive intent.

Profiling enables the delivery of highly personalised content based on inferred preferences, behavioural patterns, and emotional responses - designed to maximise engagement or commercial outcomes, potentially reinforcing behavioural patterns, influencing preferences, and narrowing exposure to information at a formative stage of development. The integration of advertising within platform design, for example through native ads or influencer content, further blurs the distinction between commercial and non-commercial material, increasing the risk of covert or manipulative advertising practices.

Research on mobile applications used by children has shown that many apps transmit data to third parties and incorporate advertising models based on behavioural tracking,⁴ often within complex adtech ecosystems involving multiple intermediaries. In practice, this makes it difficult for

² European Data Protection Board (EDPB), Guidelines 05/2020 on Consent under Regulation 2016/679 (2020), Section 7.1.

³ Rights Foundation, Pathways: How Digital Design Puts Children at Risk (2021),

<https://5rightsfoundation.com/uploads/Pathways-report.pdf>.

⁴ Reyes et al., "Won't Somebody Think of the Children? Examining COPPA Compliance at Scale" (2018), <https://petsymposium.org/popets/2018/popets-2018-0021.pdf>.

organisations to fully account for downstream data use or ensure that profiling restrictions are effectively enforced - a practice now subject to increasing restriction across jurisdictions precisely because the commercial logic it serves is indifferent to the age of the user being targeted.

Manipulative Design and Engagement-Driven Systems

Features such as infinite scrolling, autoplay, personalised recommendations, and reward-based interaction mechanisms are designed to maximise engagement, and are often supported by algorithms that continuously analyse behaviour to determine which content is most likely to maintain attention. Children may be particularly vulnerable to these mechanisms, as they are still developing the cognitive and emotional regulation skills needed to recognise persuasive design techniques or disengage from highly stimulating digital environments. For younger users, the line between a service that is enjoyable and one that is difficult to leave is often invisible, and that invisibility is frequently by design.

Although such features are often experienced as enjoyable, what maximises engagement in the short term may not be conducive to a child's long-term well-being, particularly where systems are designed to encourage prolonged use, habitual interaction, or diminished self-regulation.

Lack of Transparency and Meaningful Consent

Privacy notices and consent mechanisms typically assume a level of understanding that is not realistic for younger users. Even where

consent is formally obtained, it may not represent a meaningful or informed decision, and many forms of data processing, such as behavioural tracking or algorithmic analysis, occur in the background and are not visible to users at all. The problem is structural: the architecture of modern digital services is designed to collect data continuously and invisibly, while the mechanisms intended to inform users about that collection are static, text-heavy, and written for a legal audience rather than a human one.

For children, this gap is particularly acute. Research indicates that children frequently disclose personal information online without understanding the associated risks or how data may be reused across platforms, exposing them to risks including data misuse, identity theft, and long-term reputational harm.⁵ But the issue extends beyond individual disclosures. Children navigating digital environments are making implicit decisions about their data constantly, through every interaction, preference, and moment of engagement, without any meaningful awareness that these interactions are being recorded, analysed, and retained. Consent, in this context, is less a decision than a fiction.

AI-Driven Systems and Emerging Risks

Generative AI tools, intelligent assistants, virtual environments, and recommendation algorithms introduce more complex and less visible forms of data processing than earlier generations of digital services. When children interact with these systems, their data may be used to train models, refine predictions, or generate tailored outputs, while automated decision-making may influence what content

⁵ Idem 1.

children see, how they interact with platforms, or how they are categorised algorithmically.

What distinguishes AI-driven risks from earlier forms of data processing is not just scale but opacity. A child interacting with a recommender system or a generative AI tool has no meaningful way of knowing what data is being used, what inferences are being drawn, or how those inferences will shape future interactions.⁶ The system learns continuously from behaviour, adjusting its outputs in ways that are neither transparent nor predictable, even to the organisations deploying them. For children, whose preferences, vulnerabilities, and emotional states may be particularly legible to systems trained on vast behavioural datasets, this opacity is not a technical limitation; it is a structural condition of how these systems operate. These are not hypothetical risks. They are the foreseeable consequences of deploying systems designed for scale in environments that include children.

3. The Global Regulatory Landscape

Regulation of children's personal data and digital safety has evolved rapidly across jurisdictions. While legal frameworks differ in structure and scope, the direction of travel is consistent: regulators are moving beyond consent-based models as the primary safeguard and instead imposing design based obligations, heightened accountability requirements, and restrictions on the commercial use of children's data. This includes, in particular, obligations relating to privacy by design and by default, age-appropriate transparency, and limitations on profiling and targeted advertising involving minors. In practice, this reflects a broader shift toward **risk-based regulation**, under which organisations are expected to proactively assess and mitigate risks to children, rather than relying solely on user or parental choice mechanisms.

The table below provides a comparative overview of the key frameworks across major jurisdictions.

Jurisdiction	Primary Framework(s)	Age Threshold	Key Mechanisms	Enforcement Status
European Union	General Data Protection Rules ("GDPR") (Art. 8, Art. 25, Art. 35); Digital Services Act (DSA)	Under 16 (parental consent for information society services, GDPR Art. 8; Member States may lower to 13); under	Parental consent for information society services offered directed to children (GDPR Art. 8); data protection	Active: enforcement by Data Protection Authorities across Member States; significant fines issued ⁷ ; increasing enforcement under the DSA, particularly for large online ⁸⁹

⁶ UNICEF, Guidance on AI and Children (2025), <https://www.unicef.org/innocenti/media/11991/file/UNICEF-Innocenti-Guidance-on-AI-and-Children-3-2025.pdf>.

⁷ See Bundesverband der Verbraucherzentralen v Planet49 GmbH (C-673/17), Judgment of 1 October 2019; and Data Protection Commission, Inquiry into

Meta Platforms Ireland Limited (Instagram service) (Decision, 2 September 2022).

⁹ See Data Protection Commission, Inquiry into TikTok Technology Limited (Decision, 1 September 2023); and European Data Protection Board, Binding Decision

		18 (enhanced protections under DSA)	by design and by default (Art. 25); DPIAs where processing is likely to result in high risk (Art. 35); enhanced transparency obligations for child users; restrictions on targeted advertising based on profiling of minors (DSA); increased platform accountability obligations	
United Kingdom	UK GDPR; AADC (Age Appropriate Design Code), commonly referred to as "Children's Code"	Under 13 (parental consent required for information society services, UK GDPR Art. 8 / s.9 Data Protection Act 2018); under 18 (enhanced protections under AADC, applicable to services likely to be accessed by children)	Parental consent (UK GDPR); data protection by design and by default; high privacy defaults; data minimisation; age-appropriate transparency; restrictions on nudge techniques; DPIAs where high risk; best interests of the child (AADC)	Active: ICO enforcement, audits, and ongoing AADC compliance reviews; increasing regulatory scrutiny of online platforms and child-focused services
United States	Children's Online Privacy Protection Act ("COPPA") (federal); emerging state-level children's privacy and design codes (e.g. California Age-Appropriate Design Code, Texas SCOPE Act)	Under 13 (parental consent required for collection and use of personal data, COPPA); under 18 (enhanced protections under state-level frameworks, scope varies - e.g. California AADC, Texas SCOPE Act)	Verifiable parental consent for collection and use of personal data (COPPA); data minimisation and purpose limitation principles emerging at state level; restrictions on targeted advertising and profiling of minors	Active: FTC COPPA enforcement; increasing state-level enforcement by Attorneys General; regulatory activity expanding in relation to children's online safety and design obligations

2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR) (2 August 2023).

			under certain state laws; age-appropriate design and default privacy settings (e.g. California AADC); enhanced transparency obligations	
Canada	Personal Information Protection and Electronic Documents Act ("PIPEDA"); OPC regulatory guidance (children's privacy)	No fixed statutory age threshold; consent validity assessed based on individual capacity to understand (PIPEDA)	Meaningful consent standard; heightened protection for minors; age-appropriate transparency; regulatory focus on children's data practices	Moderate: OPC guidance active; ongoing reform discussions
Brazil	Lei Geral de Proteção de Dados Pessoais ("LGPD"); Digital ECA (2026)	Under 12 (parental consent required, LGPD/Digital ECA 2026); 12-18 (heightened protections apply)	Parental consent; best interests of the child; high privacy defaults; enhanced age assurance expectations; restrictions on profiling for commercial purposes; parental supervision tools	Active: ANPD enforcement developing; Digital ECA recently enacted
UAE	Federal Personal Data Protection Law ("PDPL"); Child Digital Safety Law	Under 13 (processing generally prohibited unless verifiable parental consent obtained, CDS Law Arts. 7 and 10); under 18 (enhanced protections apply)	Parental consent; age assurance mechanisms; data protection by design and default; enhanced transparency obligations; safeguards against harmful content and processing	Emerging: regulatory framework recently enacted; enforcement and guidance developing
Saudi Arabia	Saudi PDPL; Implementing Regulations; Saudi Data and Artificial Intelligence	No fixed age threshold (focus on legal capacity and guardian representation)	Processing in the best interests of the individual; guardian consent for minors; supplementary	Emerging: regulatory framework maturing; guidance and practice developing

	Authority (SDAIA) policies		policies for children's data; emerging regulatory expectations	
China	Personal Information Protection Law ("PIPL"); Minors' Personal Information Protection Rules ("MPRP")	Under 14 (personal data classified as sensitive, and separate parental consent is required, PIPL); under 18 (enhanced protections apply)	Separate parental consent; strict data classification requirements; enhanced protections for minors' personal information; platform obligations	Active: CAC enforcement and regulatory oversight
Australia	Privacy Act 1988; Online Safety Act; recent regulatory developments	No fixed parental consent threshold (capacity-based); under 18 (enhanced protections, Privacy Act 1988/ Online Safety Act); under 16 (minimum age for social media, sector-specific regime)	Platform obligations (content moderation, safety measures); age assurance expectations; enhanced protections for children; increasing regulatory focus on design-based safeguards	Active: eSafety Commissioner enforcement; regulatory implementation advancing
Singapore	Personal Data Protection Act ("PDPA"); Personal Data Protection Commission (PDPC) Advisory Guidelines on Children's Data (2024)	No fixed parental consent threshold; consent assessed based on capacity and understanding (PDPA); parental involvement required where child lacks sufficient capacity (minors under 21 per Singapore civil law)	Consent assessed based on child's understanding; organisational accountability; age-appropriate safeguards; parental involvement where appropriate	Moderate: PDPC enforcement active; child-specific framework primarily guidance-based

The following subsections provide additional context on the key regulatory developments within each region.

European Union and United Kingdom

In the EU, the GDPR establishes parental consent requirements for children below the applicable age threshold (up to 16, with Member State flexibility down to 13) and applies core data protection principles - including transparency, data minimisation, accountability, and privacy by design and default - with heightened importance where minors are concerned. The Digital Services Act (DSA) complements this framework at the platform level by introducing systemic risk management obligations and restricting the use of personal data for targeted advertising based on profiling minors. Recent regulatory guidance further reinforces expectations around child protection in digital environments.¹⁰

The United Kingdom has developed one of the most operationalised child-specific regimes through the Age Appropriate Design Code (AADC). Applicable to services likely to be accessed by children under 18, the Code establishes enforceable standards on default privacy settings, data minimisation, and the avoidance of design practices that exploit behavioural vulnerabilities. Enforcement by the Information Commissioner's Office (ICO) has demonstrated a shift toward proactive supervision and accountability in the design of digital services.¹¹

¹⁰ European Commission, Communication from the Commission – Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 of Regulation (EU) 2022/2065 (Digital Services Act), OJ C, 2025/5519, 14 July 2025, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202505519.

¹¹ UK Information Commissioner's Office (ICO), Children's Code Strategy Progress Update –

United States and Canada

In the United States, the Children's Online Privacy Protection Act (COPPA) remains the primary federal framework, requiring verifiable parental consent for the processing of personal data of children under 13. However, the regulatory landscape is evolving through state-level initiatives, which increasingly introduce broader protections for minors, including restrictions on behavioural advertising and emerging design-based obligations. Notably, California's Age-Appropriate Design Code Act represents a significant shift toward a risk- and design-based model applicable to users under 18, although its implementation remains subject to ongoing constitutional litigation.¹² Enforcement activity by the Federal Trade Commission (FTC) and state Attorneys General continues to intensify.

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) does not provide a fixed age threshold or extensive child-specific provisions. Instead, regulatory guidance emphasises that the validity of consent must be assessed in light of the individual's capacity to understand the nature and consequences of processing. The Office of the Privacy Commissioner (OPC) has increasingly highlighted the vulnerability of minors and is exploring the development of more tailored protections, including the potential

December 2025, 1 December 2025, available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/children-s-code-strategy-progress-update-december-2025/>.

¹² See *NetChoice, LLC v. Bonta*, No. 23-2969 (9th Cir. 2026), concerning constitutional challenges to the California Age-Appropriate Design Code Act.

introduction of a children-specific privacy code.¹³

Latin America

Brazil has emerged as a leading jurisdiction in the region by combining the general framework of the Lei Geral de Proteção de Dados (LGPD) with the recently enacted Digital Statute for Children and Adolescents (Digital ECA), which entered into force in March 2026. The framework reinforces the best interests of the child as a guiding principle and introduces enhanced obligations for digital service providers, including high-privacy default settings, stronger expectations around age assurance mechanisms beyond simple self-declaration, restrictions on profiling for commercial purposes, and tools enabling parental supervision. While enforcement practice under the new law is still developing, regulatory momentum is clearly increasing.¹⁴

Other jurisdictions in the region, such as Mexico and Argentina, continue to rely primarily on general data protection frameworks, supplemented by guidance and sector-specific initiatives. However, regulatory attention to children's online safety and digital advertising practices is growing across Latin America.

GCC and Middle East

Across the GCC, data protection frameworks are relatively recent and generally do not yet contain highly detailed child-specific regimes. Nevertheless, regulatory developments are accelerating.

The United Arab Emirates has taken a significant step with the introduction of a dedicated Child Digital Safety Law ("CDS") , which establishes a comprehensive framework addressing both data protection and broader online safety risks. The law introduces obligations relating to parental consent, age assurance, platform accountability, and the mitigation of harmful content, with particularly strict conditions applying to the processing of personal data of younger children.¹⁵

The CDS Law adopts a tiered, risk-based approach to children's data protection. A "child" is defined as any individual under 18, with enhanced protections for those under 13. In particular, Articles 7 and 10 impose strict restrictions on processing: for children under 13, platforms are generally prohibited from collecting, processing, publishing, or sharing personal data unless explicit, documented, and verifiable parental consent is obtained, coupled with clear, age-appropriate transparency obligations and mechanisms for withdrawal of consent.

¹³ Office of the Privacy Commissioner of Canada (OPC), Exploratory Consultation on the Development of a Children's Privacy Code, 2025, available at: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-children-code/expl_children-code/.

¹⁴ Autoridade Nacional de Proteção de Dados (ANPD), ANPD publica orientações preliminares e cronograma para aferição de idade no ambiente digital, 2025,

available at: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-orientacoes-preliminares-e-cronograma-para-afericao-de-idade-no-ambiente-digital>.

¹⁵ White Label Consultancy has recently published an article dedicated to this topic. It is available at: <https://whitelabelconsultancy.com/child-digital-safety-meets-data-protection-the-uaes-new-child-digital-safety-law/>.

The framework moves beyond a purely consent-based model by embedding privacy by design and by default. Children's accounts must be configured with high privacy settings by default, limiting data access to what is strictly necessary and restricting access to authorised personnel. The law also introduces strong limitations on the commercial exploitation of children's data, including prohibitions on targeted advertising and behavioural tracking for children under 13, and broader restrictions on profiling and advertising practices for all children under 18.

In Saudi Arabia, the Personal Data Protection Law (PDPL) and its implementing regulations address children's data primarily through broader concepts of legal capacity and representation. Processing of personal data relating to individuals lacking full legal capacity is generally subject to guardian involvement and must be carried out in the individual's best interests. While supplementary policies provide additional guidance,¹⁶ the framework remains less prescriptive than in some other jurisdictions.

Under the PDPL, children's data is not governed by a fixed statutory age threshold but instead through principles of legal capacity, representation, and lawful processing. Consent must be provided by a legal guardian where the data subject lacks capacity, and controllers are required to ensure that processing is necessary, proportionate, and aligned with the individual's best interests.

The implementing regulations further require controllers and processors to adopt appropriate technical and organisational measures, and to consider heightened risks associated with vulnerable data subjects. In practice, this may trigger enhanced compliance obligations, such as conducting impact assessments where processing is likely to result in high risk (e.g. monitoring, profiling, or large-scale processing involving children), and ensuring appropriate safeguards in digital services accessible to minors.

Asia-Pacific

China has established one of the most stringent and operationally detailed regimes for children's data protection. Under the Personal Information Protection Law (PIPL), personal data of children under 14 is classified as sensitive personal information, triggering enhanced protection requirements, including separate parental consent. At the same time, broader regulatory frameworks apply to minors under 18, imposing additional obligations on platforms, including age-appropriate design features, strengthened governance and compliance mechanisms, and mandatory audit and reporting requirements.

Australia is undergoing a period of significant regulatory development. In addition to existing obligations under the Privacy Act 1988 and the Online Safety Act, recent measures - including the eSafety Commissioner's guidance on age assurance,¹⁷ minimum age requirements for certain online

¹⁶ Saudi Data and Artificial Intelligence Authority (SDAIA), Children and Incompetents' Data Protection Policy, 5 May 2020, available at: <https://sdaia.gov.sa/ar/SDAIA/about/Documents/Children and Incompetents' Data Protection Policy.pdf>.

¹⁷ eSafety Commissioner, Age Verification Roadmap (2023), available at: https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification?utm_source=chatgpt.com#targeted-consultation

services¹⁸ and strengthened expectations around platform design and default settings - have introduced stronger obligations on platform responsibility. These developments emphasise age-appropriate design, risk-based safeguards, and enhanced protections for minors in digital environments

Singapore adopts a more principles-based approach under the Personal Data Protection Act (PDPA), without a fixed statutory age threshold. Instead, the validity of consent is assessed based on the individual's capacity and understanding. Recent advisory guidelines issued by the Personal Data Protection Commission (PDPC) provide additional clarity on the handling of children's personal data, emphasising organisational accountability, age-appropriate safeguards, and the role of parental involvement where necessary. Recent advisory guidelines issued by the Personal Data Protection Commission (PDPC) provide additional clarity on the handling of children's personal data, emphasising organisational accountability, age-appropriate safeguards, and the role of parental involvement where necessary.¹⁹

4. What Regulators Expect: Core Compliance Mechanisms

Despite significant variation in how jurisdictions have structured their legal frameworks, a clear pattern of convergence has emerged across regions. Four regulatory mechanisms appear consistently, and in each case, the direction of travel is the same: away

from procedural compliance and toward structural accountability embedded in how services are designed and governed.

Parental Consent and Age Assurance

Parental or guardian consent before processing the personal data of younger users remains a foundational requirement across jurisdictions, reflecting the recognition that children may lack the legal capacity or practical ability to make fully informed decisions about their personal data. In practice, implementing this requirement necessitates reliable age assurance mechanisms, and regulators are increasingly explicit that simple self-declaration is no longer sufficient. Organisations should expect growing pressure to implement more robust methods of age verification, proportionate to the risk profile of the service. At the same time, consent frameworks must include tools enabling parents to review, manage, and withdraw consent, such as parental dashboards and account controls.

Restrictions on Profiling and Targeted Advertising

Many digital platforms rely on behavioural analytics to personalise content, optimise engagement, and deliver targeted advertising. When applied to children, these practices are increasingly treated as high-risk, both because children are less able to recognise commercial persuasion, and because large-scale profiling may generate long-term digital profiles with

¹⁸ eSafety Commissioner (Australia), Social Media Age Restrictions, 2025, available at: <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions>.

¹⁹ Personal Data Protection Commission (Singapore), Advisory Guidelines on the PDPA for Children's

Personal Data in the Digital Environment, issued 28 March 2024, available at: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-pdpa-for-children's-personal-data-in-the-digital-environment_mar24.pdf.

lasting consequences. Several jurisdictions have introduced restrictions or outright prohibitions on targeted advertising directed at minors. In practice, this means that platforms cannot use data about a user's browsing behaviour, content preferences, or inferred characteristics to select or deliver advertisements when that user is, or is likely to be, a child - regardless of whether parental consent was obtained. The EU's Digital Services Act, the UK's Age Appropriate Design Code, and California's Age-Appropriate Design Code Act all reflect this approach. Recommender systems and engagement-optimisation algorithms are receiving growing scrutiny, with the scope of assessment expanding beyond advertising practices to the broader role of algorithms in shaping children's online experiences.

Privacy-by-Design and Age-Appropriate Design

Age-appropriate design is a regulatory framework that requires digital services likely to be accessed by children to be designed with the developmental needs and vulnerabilities of minors as the starting point, rather than as an afterthought. Rather than applying adult-oriented defaults and expecting children to opt out of risks, the framework inverts the logic: protective settings are the default, and the burden falls on the organisation to justify any departure from them. The UK's Age Appropriate Design Code, the most detailed implementation of this framework to date, establishes 15 standards covering default settings, data minimisation, transparency, profiling, and the prohibition of design practices that exploit children's behavioural vulnerabilities.

Child-specific safeguards must therefore be integrated directly into service design, not bolted on after deployment. This means

applying high-privacy settings by default, limiting data collection, disabling behavioural tracking or location-sharing features for younger users, and designing interfaces that discourage unnecessary data disclosure. Compliance is assessed not only at the level of policies or disclosures but at the level of product architecture and default settings - a shift that moves the compliance question from what an organisation says it does to how its service actually behaves. Age-appropriate design frameworks extend this further, requiring the avoidance of features that encourage excessive engagement or manipulate user behaviour, and placing the burden of proof on organisations to demonstrate that design choices were made with children's interests in mind.

Transparency Adapted to Children

Traditional privacy notices written in complex legal language are increasingly viewed as inadequate. Regulators expect communications to be accessible and understandable to younger users through simplified language, layered notices, visual explanations, or interactive tools. The underlying expectation is meaningful comprehension, not formal disclosure. This represents a higher bar than most organisations currently meet, and one that requires coordination between legal, product, and UX teams rather than legal drafting alone.

Risk-Based Governance and Impact Assessments

Organisations are expected to identify, assess, and mitigate risks to children proactively before services are deployed, not in response to complaints or breaches. Data Protection Impact Assessments are required in several jurisdictions where processing presents high

risk, and children's data will frequently trigger this threshold. Beyond DPIAs, regulators expect broader governance measures: internal policies addressing children's data specifically, enhanced security controls, staff training across product and engineering teams, and ongoing monitoring of live services. The emphasis is shifting toward demonstrable accountability: organisations must be able to show not only that safeguards exist, but that risks were identified and addressed at the design stage.

The Overall Direction of Travel

Taken together, these mechanisms signal a clear shift in regulatory expectations. Consent alone is no longer treated as sufficient. Children are consistently classified as a vulnerable category requiring enhanced protection by default, and certain data uses - behavioural profiling, targeted advertising, engagement-driven design - are becoming increasingly difficult to justify where minors are involved regardless of consent. Organisations are no longer assessed solely on whether they comply with formal legal requirements, but on whether they can demonstrate that services are designed and operated in a way that actively protects children. For organisations operating across jurisdictions, the key challenge is therefore not only to understand individual legal obligations, but to translate these converging expectations into consistent governance frameworks and product design principles that hold across markets.

5. Cross-Border Compliance Challenges

The convergence of regulatory principles described in the previous section does not translate into a uniform global framework. While regulators across jurisdictions are

moving in the same direction toward design-based obligations, risk-based accountability, and restrictions on commercial data use involving minors, the legal details differ considerably. Age thresholds, consent requirements, enforcement structures, and the scope of digital safety obligations vary in ways that create substantial operational complexity for organisations designing services that may be accessed by children across multiple markets.

One of the most immediate challenges arises from divergent age thresholds. Legal frameworks define children differently, which directly affects when parental consent requirements apply and when enhanced safeguards must be implemented. Under the GDPR, parental consent requirements may apply to children under 16, whereas COPPA applies to children under 13, and China's PIPL sets the threshold at under 14. These variations make it difficult to design a single, uniform compliance approach across markets. Organisations must either align to the most restrictive applicable threshold or maintain jurisdiction-specific configurations that add operational complexity.

Closely related are differences in parental consent and age assurance requirements. While many frameworks rely on parental consent as a core safeguard, the standards for obtaining and verifying such consent vary considerably. Some jurisdictions require verifiable parental consent supported by specific authentication methods; others provide more flexibility. Similarly, expectations around age verification are evolving rapidly, with regulators increasingly requiring more robust mechanisms beyond simple self-declaration. Organisations must therefore implement flexible consent management systems capable of adapting to differing legal and technical requirements across markets.

Fragmentation also extends to enforcement and regulatory interpretation. Multiple authorities, including data protection regulators, consumer protection agencies, and sector-specific bodies, may have overlapping jurisdiction over children's digital safety within the same market. Enforcement priorities and interpretations of legal obligations can vary across jurisdictions even where underlying legal principles are similar, creating uncertainty for organisations seeking to assess risk exposure and implement consistent governance practices.

International data transfers introduce an additional layer of complexity. Many digital services rely on global infrastructure involving cross-border data flows for storage, analytics, and service delivery. Data protection frameworks often impose restrictions on international transfers, particularly where adequate safeguards are not in place. When children's data is involved, regulators may apply heightened scrutiny given the increased sensitivity of processing minors' personal information.

In practice, organisations increasingly adopt risk-based strategies that apply the most protective standards across jurisdictions, supplemented by local adaptations where necessary. This may include implementing higher default privacy settings globally, limiting profiling activities across all markets, or applying stricter consent and age assurance mechanisms as a baseline. These challenges underscore the importance of integrated governance approaches that combine legal analysis, product design, and operational controls. Ultimately, children's data protection must be treated as a cross-functional priority rather than a jurisdiction-specific compliance task.

6. Practical Compliance Framework for Organisations

The following framework provides a structured sequence for organisations seeking to embed child-specific safeguards into the design, development, and operation of digital services. The steps are ordered by implementation logic: from initial assessment through to ongoing governance and transparency, each building on the foundation established by the previous.

Assess Whether Services Are Likely to Be Accessed by Children

The first step is determining whether a digital service is likely to be accessed by minors. This assessment must go beyond whether the service is explicitly directed at children, as regulatory obligations may apply to any platform reasonably likely to attract younger users regardless of its primary intended audience.

Organisations should evaluate the demographics of their user base, the nature and functionality of the service, and how it is marketed or presented. Services featuring social interaction, gaming, entertainment, or educational content carry a higher likelihood of child access. Where there is reasonable likelihood of child access, enhanced safeguards should be implemented even in the absence of explicit child-directed design. The assessment itself should be documented as part of the organisation's accountability record.

Map Children's Data Processing Activities

Once child access has been identified, organisations should conduct a comprehensive review of how children's personal data is collected, processed, and shared within the service. This involves identifying all categories of data collected, including registration details, location data, behavioural data, device identifiers, and user-generated content, and mapping how that data flows through internal systems and to any third-party processors or service providers.

Data mapping serves multiple purposes: it identifies risk points, ensures that safeguards are applied throughout the data lifecycle, and supports compliance with accountability and transparency obligations. It also provides the factual foundation for the impact assessments and governance measures that follow.

Conduct Child-Specific Data Protection Impact Assessments

Where processing activities present increased risk, and children's data will frequently meet this threshold, organisations should conduct Data Protection Impact Assessments specifically calibrated to child-related risks. A generic DPIA is insufficient. The assessment should evaluate how product features, data collection practices, and algorithmic systems may affect children's privacy and well-being specifically, including recommender systems, engagement mechanisms, and AI-driven personalisation features.

Critically, the output of the DPIA should directly inform product and design decisions. A DPIA that sits as a compliance document divorced from development processes provides accountability on paper but not in

practice, and regulators are increasingly able to distinguish between the two.

Implement Age-Appropriate Design Principles

Organisations should integrate age-appropriate design principles into service development from the outset. Practical measures include applying high-privacy settings by default for younger users, limiting data collection, restricting behavioural tracking, and ensuring that children's accounts benefit from enhanced protections without requiring manual configuration.

User interfaces and communications should be adapted to younger audiences through simplified privacy notices, visual explanations, and contextual disclosures that help children understand how their data is used. Design choices should also actively discourage excessive engagement. Features such as autoplay, infinite scroll, and reward-based interaction mechanisms warrant particular scrutiny where children are likely to be present.

Review Advertising, Profiling, and Algorithmic Systems

Organisations should assess how behavioural data is used in services where children may be present. This means evaluating whether profiling and targeted advertising practices are applied to minors, whether those practices comply with applicable legal restrictions, and where restrictions apply, whether technical controls are in place to enforce them rather than merely policy commitments.

Recommender algorithms and engagement-optimisation systems should be reviewed specifically for their interaction with younger users. Algorithms designed to maximise

engagement may inadvertently expose children to inappropriate content or reinforce harmful usage patterns. Regular algorithmic audits with child-specific risk criteria are becoming an expectation rather than a best practice in leading jurisdictions.

Strengthen Governance Structures and Internal Accountability

Effective protection of children's data requires governance structures that ensure privacy and safety considerations are embedded in organisational decision-making, not handled solely by legal or compliance teams. Organisations should establish policies specifically addressing children's data, implement training programmes across product, engineering, marketing, and customer support functions, and assign clear ownership for child-specific compliance obligations.

Governance frameworks should also include ongoing monitoring mechanisms. Live services must be reviewed regularly to identify emerging risks, changes in user demographics, or new product features that may affect children. Accountability is not a one-time exercise at launch. Regulators increasingly expect evidence of continuous oversight, and the absence of monitoring is itself treated as a governance failure in several jurisdictions.

Provide Transparency and Parental Control Tools

Meaningful parental involvement requires more than making tools available. Organisations should implement mechanisms that allow caregivers to actively monitor and manage children's interactions with digital services, including account controls, content filters, screen time management, and clear

processes for withdrawing consent or requesting data deletion. The test is whether a non-technical parent can meaningfully exercise oversight, not whether the tools technically exist.

Privacy notices should be presented in formats accessible to both children and their caregivers. For parents, this means clear information about what data is collected, how it is used, and what controls are available. Layered notices, offering a simple summary with the option to access more detail, are particularly effective for audiences spanning both children and adults.

7. Strategic Opportunities - From Reactive Compliance to Safer Product Design

Regulatory developments around children's data are typically framed as compliance burdens. The more useful framing is different: organisations that move beyond reactive compliance and embed child-centric safeguards into product design are likely to be better positioned both from a risk and a commercial perspective. The shift creates five distinct strategic opportunities.

Compliance as a Product and Design Function

Requirements such as age-appropriate design, high-privacy defaults, and restrictions on profiling cannot be implemented through policies or contractual controls alone. They require changes to system architecture, default configurations, user interfaces, and product decision-making processes. Organisations that integrate privacy, legal, and product teams early in the design lifecycle are better equipped to meet regulatory

expectations and to avoid the significantly higher cost of redesigning services after deployment.

For organisations in sectors with high child engagement, including gaming, edtech, social platforms, and connected devices, this integration is not optional. Regulators in leading jurisdictions are already examining product architecture and default settings as primary evidence of compliance, not as secondary considerations. Treating child-centric design as a product function rather than a legal afterthought is the structural shift that makes sustainable compliance possible.

Trust as a Competitive Differentiator

As public awareness of children's digital safety increases, parents, institutional buyers, and regulators are placing greater weight on how platforms protect younger users. Services that demonstrate clear safeguards, including transparent data practices, reduced reliance on behavioural tracking, and meaningful parental controls, are increasingly differentiated in markets where trust has become a purchasing criterion.

This is particularly relevant in edtech and family-oriented consumer services, where procurement decisions are often made by parents or institutional buyers who apply safety and privacy criteria explicitly. Organisations that can demonstrate compliance with demanding frameworks such as the UK Age Appropriate Design Code or California's AADC signal a level of product maturity that extends beyond regulatory minimum requirements.

Global Standardisation as Operational Simplification

The fragmentation of children's data regulation across jurisdictions creates compliance complexity, but it also creates an opportunity. Organisations that implement a single baseline aligned with the most protective global standards, rather than managing jurisdiction-specific configurations, reduce operational complexity while achieving compliance across markets simultaneously.

In practice, this means applying the strictest applicable age threshold globally, implementing default privacy settings that meet the highest bar across jurisdictions, and building consent and age assurance mechanisms robust enough to satisfy both EU and US requirements. The upfront investment in a higher global standard is typically lower than the ongoing cost of maintaining multiple jurisdiction-specific product variants, and significantly lower than the cost of enforcement action in multiple markets.

Governance Synergies Across Risk Domains

Structured frameworks for assessing risks to children, including impact assessments, algorithmic audits, and design reviews, create governance infrastructure that transfers directly to other high-risk areas. Organisations that develop rigorous processes for evaluating how services affect vulnerable users are better placed to address adjacent regulatory requirements: AI governance obligations, sensitive data processing, and the emerging platform accountability frameworks taking shape across jurisdictions.

Child-centric governance is therefore not a siloed compliance function. It is an early investment in the risk management

capabilities that regulators are extending progressively across the digital economy. Organisations that build these capabilities around children's data protection will find them directly applicable as broader obligations mature.

Preparedness for the Next Regulatory Wave

The regulatory trajectory is clear. Expectations applied to services accessible to children are consistently ahead of those applied to the broader digital economy, and they consistently predict where general platform regulation is heading. Privacy-by-design, algorithmic accountability, restrictions on engagement-driven design, and proactive risk assessment were all established as child-specific requirements before becoming general regulatory expectations. AI governance frameworks now emerging across jurisdictions reflect the same logic.

Organisations that have already embedded child-centric safeguards into their design and governance processes will require fewer structural changes as these obligations extend to broader user populations. Those that have not will face the same transition at greater cost, under greater regulatory pressure, and with less time to adapt. The strategic case for acting now is not only about managing current compliance risk. It is about building the organisational capability to navigate a regulatory environment that will continue to tighten, and doing so from a position of design maturity rather than reactive adjustment.

8. Conclusion - Navigating Children's Data Protection and Digital Safety Globally

Across jurisdictions, a set of core principles governing the protection of children's personal data is becoming increasingly stable. Children are consistently classified as a vulnerable category requiring enhanced protection by default. Consent alone is consistently treated as insufficient. Behavioural profiling, targeted advertising, and engagement-driven design practices are subject to heightened scrutiny, and in a growing number of jurisdictions, to outright restriction. Transparency must be meaningful and adapted to younger audiences, not merely formal. Product design is now a primary site of compliance assessment, not a secondary consideration. These principles hold regardless of how specific legal requirements differ across markets, and organisations can treat them as a reliable foundation for governance and product decisions.

The translation of these principles into specific legal obligations, however, remains uneven. Age thresholds, consent standards, enforcement structures, and the scope of digital safety obligations differ considerably across jurisdictions, creating genuine complexity for organisations operating internationally. This unevenness is not a sign that convergence is failing, it reflects the reality that regulatory frameworks develop at different speeds and through different institutional structures. The direction is consistent; the pace and detail vary. For organisations, this means that designing to the highest applicable standard across markets is both the most protective and, over

time, the most operationally efficient approach.

The trajectory of that convergence points clearly toward broader platform accountability. Requirements that began as child-specific, including privacy-by-design, algorithmic accountability, restrictions on manipulative design, and proactive risk assessment, are consistently extending to the wider digital economy. AI governance frameworks now taking shape across jurisdictions reflect the same logic: platforms bear responsibility for the effects of their systems on users, not only for the data those systems collect. Children's data protection has functioned, and will continue to function, as the leading edge of this shift.

For organisations operating digital services, the practical implication is straightforward. Embedding child-centric safeguards into product design, governance frameworks, and operational controls is not only a response to current regulatory requirements. It is preparation for a regulatory environment that will continue to tighten, and an investment in the organisational capability to navigate that environment from a position of design maturity rather than reactive adjustment. Organisations that make this investment now will be better positioned to manage regulatory risk, build user trust, and operate responsibly in digital ecosystems increasingly shaped by child protection and digital safety regulation.

White Label Consultancy works with organisations at this intersection, helping translate converging regulatory expectations into governance frameworks, product decisions, and operational controls that hold across jurisdictions.

Authors



Nicholai Pfeiffer

Managing Partner

White Label Consultancy

np@whitelabelconsultancy.com



Dr. Magdalena Góralczyk

Data Protection Partner

White Label Consultancy

mg@whitelabelconsultancy.com



Nauani Benevides

Associate

White Label Consultancy

nbe@whitelabelconsultancy.com



Darya Ghasemzadeh

Associate

White Label Consultancy

dgh@whitelabelconsultancy.com

Contact

hello@whitelabelconsultancy.com

+45 71 74 74 54

NORWAY

Main Office Oslo

 +47 4141 2168

 Fjordalléen 16
0250 Oslo

DENMARK

Copenhagen Office

 +45 71 74 74 65

 Dampfærgevej 27
2100 København Ø

POLAND

Warsaw Office

 +48 515 07 99 77

 Ul. Marszałkowska 58/15
00-545 Warszawa

UNITED ARAB EMIRATES

Dubai Office

 +971 50 4536616

 Dubai World Trade Center
Dubai

WHITELABELCONSULTANCY.COM

