Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Protecting Children's Data Privacy

POLICY PAPER I

International Issues And Compliance Challenges

October 20, 2022

Table of Contents

Executive Summary **3**

Foreword **6**

I. Introduction **8**

II. The Public Policy Backdrop **12**

A. Countries' Renewed Efforts to Address Children's Digital Privacy 12

B. An Emerging International Perspective: The Best Interests of the Child 14

C. An Opportunity for a New Approach to Protecting Children's Privacy 15

III. Consent **18**

A. Age of Consent 18

B. Who May Consent on Behalf of the Child? 21

C. Consent and Legitimate Interests 24

IV. Age Assurance **28**

A. The Role of Age Assurance in Protecting Children 28

B. Privacy Issues Raised by Age Assurance Solutions 29

C. Artificial Intelligence for Age Assurance 31

V. Profiling for Targeting to Children **33**

VI. Providing Transparency About the Use of Children's Data **35**

VII. A Risk-based Approach to Children's Data Privacy **39**

VIII. Conclusion **41**

Appendix One: Survey of Laws and Regulations in Key Jurisdictions **43**

Appendix Two: National Law Affecting Children's Data Privacy **57**

Appendix Three: Select Codes of Conduct and Regulator Guidance **62**

Appendix Four: Age of Consent and Verification of Consent Requirements **65**

References **70**

Executive Summary

This paper establishes the foundation for the Centre for Information Policy Leadership's work to understand and address the **difficult policy issues and regulatory and compliance challenges** organizations and data protection authorities face when addressing children's online data privacy. We identify and explore these key issues and challenges in the context of globally divergent standards and requirements and other rights and interests of children in the online environment. This first paper will be followed by a second policy paper that will focus on **practical solutions** to the issues challenges identified in the present paper.

Complying with an increasing number of laws and implementing measures to address children's data privacy in the global market is a complex undertaking. Moreover, laws to address children's data privacy do not operate in a vacuum—their obligations must be met and reconciled with requirements to protect children from harm and ensure that children can access resources and participate online in ways appropriate for their age and maturity.

The issue of children's data privacy must also be considered in the context of policy developed by international organizations and individual countries, which recognizes both the importance of children's online engagement and the risks they may encounter online. International conventions, national guidance, and codes of practice increasingly identify "the best interests of the child" as the central consideration in determining how to protect children and promote an online experience that benefits them. This orientation offers an important opportunity to develop policy that is creative and effective, and that will result in enhanced opportunity and potential for children's positive online engagement.

In this paper we discuss the following key issues and challenges:

Consent. Protecting privacy in children's data raises questions about when a child has reached an age at which they can provide valid consent to the collection and processing of their data, and when a parent or other responsible adult must provide such consent.

- *Age of Consent*. The age of consent varies across jurisdictions. These differences present significant compliance challenges for organizations and inconsistent protections for children.
- *Who May Consent on Behalf of a Child*. Requiring the consent of a parent to the collection or processing of data when a child is not of age raises its own set of issues both for organizations and for families. When laws broaden the definition of "parent" to include other responsible adults who can act in their place, companies face challenges when attempting to confirm that the person can legitimately act in that capacity.
- *Consent and Legitimate Interests*. In some jurisdictions, consent is not the only basis for the lawful collection and processing of data. Some laws and regulations provide that data may be processed to further an organization's "legitimate interests." Under what circumstances might "legitimate interests" serve as the basis for processing of children's data? What analysis should be applied to make that determination?

Age Assurance. Age assurance tools attempt to address the imperative of keeping children safe online, but most age assurance methods create their own privacy issues. They also suffer from a lack of consensus among regulators globally as to whether they are effective, appropriate and support compliance with data protection law. Age assurance that relies on artificial intelligence promises greater effectiveness, but raises potential privacy concerns related to profiling, transparency, and accuracy.

Profiling for Targeting to Children. Use of profiles for targeted advertising raises concerns about children's privacy, but profiling can also enable personalized services, content and products, and help provide protections for children – for example, by helping to direct children of identified ages or age ranges away from potentially harmful environments and material toward appropriate sites. Clarity and greater legal certainty about what profiling is appropriate, in what circumstances, and by what methods would benefit organizations' compliance efforts and enhance protections for children.

Transparency About the Use of Children's Data. Enhancing and tailoring transparency for children and adults about the use of children's data will require greater understanding of what information they want and need, and when and how to best make it available. It will also require understanding what communicates to children at various stages of their development, and to adults who may have limited familiarity with technology and the online environment.

Benefits of a Risk-based Approach. A risk-based approach could shift the burden of protecting children's data away from parents (via consent) to companies that would assess and mitigate the potential harm to which data collection and processing might expose children. To be workable, such an approach would need to be thoughtfully designed and implemented across different companies' products and services aimed at children. It would need to provide for careful balancing of the benefits and risks raised by the use of children's data, and depend on clear articulation of criteria for data protection impact assessments.

Foreword

This paper is intended to serve as a foundational document for the work of the Centre for Information Policy Leadership's[1] (CIPL)on children's online privacy to explore ways to meet the data protection and compliance challenges that organizations face. **This first paper, Policy Paper I, examines issues central to children's data privacy and the challenges they raise for companies, regulators and families.** This paper **will be followed by a second paper** titled *Protecting Children's Data Privacy Policy Paper II: Practical Solutions to Protect Children and Enhance Compliance* (working title), **which will highlight existing and potential policy, industry sector and technology solutions** that can address them.

Policy Paper I frames the issues, highlighting the growing concerns of policymakers about children's data privacy and their shift in orientation from merely protecting children from dangers in an unregulated space toward one that places data protection in the context of empowering children to exercise their right to participate online and promoting their best interests. It considers the wide disparity in requirements for consent to collection and processing of children's data and the impact that variation has on organizations' efforts to comply with laws across jurisdictions. It also discusses age assurance methods, and the tension that exists between the need for relative certainty about age and concerns about the collection of data necessary to provide that certainty.

The paper looks at the potential and challenges involved in providing meaningful transparency about data collection and processing for children and their families. Finally, it discusses proposals to protect children's data based on risk/benefit assessment and mitigation and the issues such an approach may raise.

The four appendices in the paper provide information that illustrates the compliance challenges central to policy discussions about protecting children's data. **Appendix One** provides a brief review of some of the laws and regulations established in countries around the world to protect the privacy of children's data. These reviews primarily focus on provisions related to the age at which individuals can provide valid consent, when the consent of a parent or guardian is required, and steps that must be taken to verify that

consent. They note when age alone is not sufficient or is not the only relevant consideration in establishing valid consent, and where additional evaluation, e.g., with respect to a child's intellectual development or maturity, are required. Where relevant, they note requirements specifically directed at data collected in the context of education, as well as additional general provisions related to transparency, and to data access and erasure.

Appendix Two provides an overview of national legislation in table form to enable easy comparison of requirements across jurisdictions.

Appendix Three highlights some of the codes of conduct, best practices and industry guidance that have been articulated by data protection authorities. These illustrate policymakers' and regulators' shift from an emphasis solely on data protection to a more holistic approach that places children's data privacy in the context of the need to keep them safe and promote their positive online experience.

Appendix Four provides in table form an overview of the various ages of consent and consent requirements across jurisdictions.

The reviews provided in the Appendices highlight the wide variation in these laws and codes in their compliance requirements and the kinds of protection they afford. They reflect the varied understanding and attitudes across cultures and jurisdictions about when minors can understand the consequences of data collection and processing—and therefore possess the capacity to act on their own behalf—and when the participation and consent of an adult should be required.

It is important to note that **this document is designed to identify issues for possible consideration in future work.** While it is intended to inform the ongoing discussion about children's data privacy, this Policy Paper I does not attempt to resolve questions and challenges. Rather, it seeks to establish the foundation for CIPL's Policy Paper II, which will examine existing and potential solutions and innovative technology and policy measures that can address these challenges. While each of the issues raised in this paper merit deep exploration, this paper addresses them at a higher level to place them in the broad context of the challenges that protecting children's privacy online raises. It anticipates in-depth discussions among policymakers, organizations, regulators and experts about how these issues can be addressed in a way that serves children and their families and promotes robust compliance and the positive experience of children in a global digital environment. **Some organizations have already made significant investments in the protection of children's privacy and safety and have put in place meaningful measures to address these issues. These measures, and other proposals for solutions, will be discussed in CIPL's Policy Paper II.**

I. Introduction

The digital environment has become a place where individuals build community, access information, learn, play, research, work, shop, create, collaborate, visit their health care provider, express ideas and opinions, and participate in public life. **Children and teens, who represent one-third of all Internet users**,[2] participate in the digital world at the earliest stages of life.

Young people access online resources for education—to participate in virtual classrooms, access e-books, research areas of study, complete and submit homework, and collaborate with classmates. The Internet provides unique benefits and opportunities for children to express themselves and makes available to them a vast quantity of information at an instant. It has become a place where children play, meet each other socially and gain the skills necessary to be responsible and confident digital citizens. Like their parents and adult caregivers, children now often also receive medical care online. As they mature, online resources provide them with critical resources and support related to such sensitive issues as mental health, gender identity and domestic violence. And the pace of migration of children's life online has only increased recently, as the Covid-19 pandemic has made it necessary that still more aspects of their lives—including their interactions with extended family, and their engagement in communities beyond school, such as worship and youth groups—happen online.

Adults' and children's ability to participate online requires the collection and processing of data—some of it personal. While the gathering and use of personal data makes many of the benefits of the Internet and digital technology possible, it also raises risks. The collection, storage and processing of children's data of all kinds raises concerns about their privacy and the potential exploitation of their specific vulnerabilities when they engage in commercial activity, particularly when it occurs without appropriate protection and countervailing benefits for the child. It also raises worries about the creation of profiles that may follow them into adulthood.

Protecting children's privacy in the digital world, particularly as technologies emerge and develop rapidly, therefore raises complex issues, and requires reconciling competing concerns. Solutions in law, technology and policy must take into account the following:

- ***Children have the right to participate in and reap the benefits of the online world.*** Children need—and have the right—to reap the benefits of digital technology. Solutions to children's data privacy should respect children's rights to readily access resources and participate in online activities appropriate for them, to express themselves, and to develop their online autonomy.
- ***The global nature of the Internet presents challenges for companies*** who must comply with data protection requirements across many jurisdictions, and for users who rely on global networks to access content and participate online. One of the most significant benefits of the Internet is the access it provides to people, resources and markets around the world. However, organizations operating across geographies and jurisdictions face the challenge of meeting diverse and often conflicting legal requirements. Similarly, children and their families must navigate an online environment where protections are sometimes inconsistent and often unclear.[3]
- Children's ability to understand the risks and consequences of data collection change as they grow. As children develop and mature, their ability to understand the implications of data collection and processing changes as well. These changes affect considerations for the appropriate age of consent—at what age should children be able to provide consent and whether that age should depend upon the nature and purpose of the data collection. Measures to address issues of children's privacy must reflect this reality and accommodate the way children mature over time.
- ***The nature of the material and activities children need and should have access to also changes as they mature.*** Children's need for access to information and online engagement changes and potentially increases as they mature. As they enter adolescence, for example, children may need to access materials about sensitive matters they may not be comfortable discussing with their parents. At the same time, their psychological maturity and need to learn to exercise personal autonomy also grow. Just as in the physical world, children and teens need the opportunity to understand and navigate risks and to develop their ability to make good decisions about where and how they spend time online and with whom.[4]

- ***The need to collect data to verify that children are of an appropriate age raises its own privacy issues.*** Making determinations about whether a child is of the required age to share their data, access materials or participate in an activity online raise questions of age verification. Age verification methods, in turn, require collection and processing of data and raise their own privacy concerns, as well as issues of inclusion, data minimization and accuracy.[5]
- ***Children require protection from inappropriate content and online bullying and predation.*** Issues related to protection of children's privacy cannot be addressed in a vacuum. Measures to protect children's data must accommodate the need to keep them from accessing content not appropriate for them, to protect from predatory adults, and to shield them from other children who may be engaging in harmful activities. Children's safety is, of course, of utmost importance. However, rules to provide protections from these harms are not the remit of data protection law and regulators, and they affect—and complicate—organizations' compliance responsibilities.
- ***Parents and caregivers are responsible for protecting children from online harm and guiding their online experience.*** Just as parents are responsible for their children's wellbeing in the physical world, they also are concerned about protecting their children from online harm. Tensions may exist between a parent's desire to protect their child's privacy and their child's need to share data to engage in digital life in a way that is appropriate to their age and maturity.[6] Parents' desire to help their children reap the benefits available to them online and to supervise their children's online activities is challenged by the parents' relative lack of familiarity with and ability to meaningfully navigate new technologies, platforms and data uses—particularly relative to their children's sophistication with digital environments.[7]

These competing concerns complicate policy discussions about children's data privacy. Protecting children's data in a way that accommodates these interests has prompted the development of guidance that attempts to incorporate a dynamic analysis designed to promote the *best interests of the child*. This guidance[8] takes into consideration a child's age, their evolving maturity and developmental needs and their capacity to understand the consequences of sharing their data, what is being offered to them, the nature of the processing, and the risks and benefits of the processing. It takes into account the need to keep children safe online, and sensitivity to the issues raised by age-verification measures which make that possible. It requires respecting the concerns of families about the collection and processing of their children's data, and their children's online safety. But it also involves the need to promote children's right to participate in digital life, recognizing that online engagement is necessary to their ability to grow and flourish.

The complexity of this analysis will require policymakers and regulators to develop and enforce effective and workable measures at the place where privacy, safety and wellbeing intersect. Such measures must also be designed in a way that organizations can practically implement them, and parents and guardians can understand and navigate them. More work is needed to identify ways these competing interests can be reconciled that serve the interests of children and their families and help organizations comply, without introducing broader surveillance.

The discussion below attempts to examine these challenges and to provide the starting point for productive discussions. CIPL's Children's Privacy Project will explore existing and anticipated solutions in Policy Paper II, to be released next year.

II. The Public Policy Backdrop

A. Countries' Renewed Efforts to Address Children's Digital Privacy

Concerns about the risks raised by children's online engagement, the collection and processing of children's data, and the impact on children's privacy have drawn the attention of governments and international organizations.

Publication of the **UK** ICO's enforceable *Age Appropriate Design Code*, the **Irish** Data Protection Commissioner's *Fundamentals*, and the **French** CNIL's *The Digital Rights of Children*, and guidance issued by data protection authorities across Europe and in **Asia** (discussed in Appendix II) highlight the importance policymakers and regulators place on children's privacy and the need to protect children online.

In addition to these measures, in May 2022, the European Commission released a new *European Strategy for a Better Internet for Kids*.[9] The strategy is designed to support implementation of EU legislation on child safety, including the Audio-visual Media Services Directive,[10] the EU's GDPR,[11] the provisions on child online safety in the Digital Services Act (DSA)[12] and a new proposal for EU legislation to protect children against sexual abuse.[13] The goal of the strategy is to facilitate the development of comprehensive EU code of conduct on age-appropriate design, building on the framework provided in the DSA.[14]

In Latin America, **Brazil** recently enacted the General Data Protection Law (LGPD),[15] which states that, "[t]he processing of personal data of children and adolescents shall be carried out in their best interest". It also provides that, "[t]he processing of personal data of children shall be carried out with the specific and prominent consent given by at least one parent or legal guardian",[16] and sets out requirements for verification of parental consent.[17] It also specifies that controllers may not condition the participation of a child in an online activity on their providing personal data beyond what is strictly necessary.[18]

In January 2022, **US** President Joseph Biden expressly called for protections for children's privacy in his State of the Union address. "It's time to strengthen privacy protections, ban targeted advertising to children, demand tech companies stop collecting personal data on our children". He also cited the need to improve children's overall mental health and well-being, and to hold social media platforms accountable for their practices. In June 2022, The American Data Privacy and Protection Act was introduced before the US House of Representatives.[19] While the legislation is designed to govern all personal data, it would supplement the Child Online Privacy Protection Act and contains special provisions focused on children and minors.[20]

Also in the US, the state of **California** passed into law the California Age Appropriate Design Code Act,[21] which places new legal obligations on companies with respect to online products and services that are "likely to be accessed by children" under the age of 18. The Act is modelled on the UK Age Appropriate Design Code and applies to businesses that provide an online service, product or feature "likely to be accessed by children" under the age of 18. The Act also establishes the California Children's Data Protection Working Group, consisting of experts in children's data privacy, physical and mental health, computer science and children's right, which will study and report to the legislature best practices for implementing the Act. The Working Group will consist of experts in children's data privacy, physical health, mental health and well-being, computer science, and children's rights.

In **Canada**, recently proposed changes to federal privacy law also aim to address children's privacy more directly. In June 2022, the Government of Canada proposed a new federal private-sector privacy law under Bill C-27 which, if passed in its current form, would expressly deem personal information of minors to be "sensitive," such that it would have to be expressly considered in operationalizing various requirements under the Act.[22] Additionally, Bill C-27 grants children more expansive rights to have their personal information deleted, and it authorizes children themselves to exercise their rights and recourse provided under the Act.[23] At the provincial level, **Quebec**'s recently amended private sector privacy legislation, which comes into force in September 2023, specifically requires parental consent for collection of data from minors under the age of 14 unless such collection clearly benefits the minor.[24] The fact that data relates to a minor must also be taken into account when responding to a request to de-index or cease disseminating information.[25]

B. An Emerging International Perspective: The Best Interests of the Child

In March 2021, the United Nations Committee on the Rights of the Child issued *General comment No. 25 on children's rights in relation to the digital environment*.[26] That document provides guidance on relevant legislative policy and other measures to ensure full compliance with obligations under the Convention on the Rights of the Child in light of the opportunities, risks and challenges in promoting and respecting children's rights in the digital environment. It highlights privacy as "vital to children's agency, dignity, and safety", and essential to their ability to exercise their rights. It notes the threats to children's privacy that may arise from data collection, and from children's own activities and the activities of their families and peers. It urges states to take legislative, administrative and other measures to ensure children's privacy is respected.

Significantly, this discussion of children's privacy is set within the broader set of interests and rights—among them the best interests of the child, the child's right to life, survival and development, and respect for "the evolving capacities of the child" and "their gradual acquisition of competencies, understanding and agency". **Privacy is noted as one of several civil rights and freedoms enjoyed by children, including access to information, freedom of expression and freedom of association.** It states that, "[p]rivacy and data protection legislation and measures should not arbitrarily limit children's other rights".

In 2021, the United Nations General Assembly published *Artificial intelligence and privacy, and children's privacy*.[27] The document sets forth principles and recommendations on children's data privacy. Significantly, these state that children are entitled to human rights and freedoms. They note that "[c]hildren's rights are universal, indivisible, interdependent and interrelated. Their right to privacy enables their access to other rights critical to developing personality and personhood, such as the rights to freedom of expression and of association and the right to health, among others".

The document also highlights **competing interests in tension when considering children's privacy**. It notes that "[t]raditionally, the privacy rights of children have been regarded as an issue for adults to determine. Children's privacy needs, however, differ from and can conflict with those of adults". It also notes that **adults' understanding of what children need with respect to privacy can "impede the healthy development of autonomy and independence and restrict children's privacy in the name of protection".**[28]

An earlier UNICEF document, *Children's Online Privacy and Freedom of Expression: Industry Toolkit*, published in 2018[29], also signals a **shift in focus in the policy discussion about children's online experience from the imperative to protect children from**

harmful content and the dangers of the online environment to the importance of empowering them to exercise their rights online. According to the document, these include privacy and freedom of expression. It considers how these rights—recognized in the United Nations Convention on the Rights of the Child (CRC)[30]—are realized in the digital world.[31]

> **Practical Challenge: Balancing the privacy of young people as they grow and mature and the interest of parents in supervising their child's online activity.**
>
> Balancing the data privacy rights of minors participating in online activities and parents' interest in overseeing their children's online activity presents companies with practical compliance challenges, particularly as children mature. The level of parental supervision necessary and appropriate when a child is five (when children require close supervision) differs markedly from that necessary when the child is 15 (when a teenager needs to learn to exercise judgment and greater autonomy when navigating the online environment).
>
> In attempting to balance the interests of the parent in supervising their child with the child's need to develop and exercise greater self-determination as they grow and develop, companies are faced with reconciling considerations and judgments that are often personal to individual families. This is especially true when making these determinations about long-time users who may first access a service as a pre-teen and continue to do so in early adulthood. Little guidance is available to help companies strike the appropriate balance.

C. An Opportunity for a New Approach to Protecting Children's Privacy

The developments discussed in this section suggest a shift in how policymakers approach the question of children's data privacy. Where the orientation once had been solely toward the protection of children from dangers that may exist in an unregulated sphere, the growing recognition of the rights of the child, and the imperative that children be empowered to exercise those rights, has broadened—and complicated—the discussion. **Increasingly, policy discussions focus on how protections should promote "the best interests of the child".**

Assessing the best interests of the child, and making determinations about children's privacy in that context, can be a complex undertaking. The need to reconcile competing interests—in privacy, in keeping children safe,[32] in children's rights to free expression and association, and in their need to participate online to access information critical to their

education, leisure, play, health and psychological development suggests that solutions will require a holistic and integrated approach.[33] Children's evolving level of maturity, capacity for responsible decision-making and need for autonomy develop over time, and call for privacy solutions designed to accommodate those changes and guidance about how those solutions practically may be implemented.

Emerging laws designed to address children's rights and risks also highlight the reality that solutions to questions of children's privacy must reflect the global nature of the Internet. The review found in the Appendices of this paper illustrates the variation in ways in which countries around the world address children's privacy in law, regulation and guidance. The discrepancies across jurisdictions in the appropriate age of consent,[34] when exceptions to consent requirements may be made,[35] and when bases for lawful processing other than consent are available, and who may act in the capacity of a parent for purposes of granting consent,[36] provide important examples of how children's privacy laws challenge the resources of companies that must build compliance into products and platforms to meet these different standards. They also highlight the challenges parents and guardians face when navigating this varied landscape with their children.[37]

Harmonization of regulatory requirements and the design of technical solutions—perhaps through recognized codes of conduct or best practices—could help businesses comply and establish for parents and children consistent, understandable protections in the digital environment. **Cultural differences and varied attitudes about children's privacy and how their online experience should be shaped and overseen will test efforts toward such harmonization.** Moreover, the need to accommodate the varying nature of digital services and advances in innovation argue for solutions that are principles based and technology neutral.

At the same time, the shift toward "the best interests of the child" as the basis for companies' decisions about children's data privacy presents its own challenges. While a consent-based approach arguably provides companies with at least some clarity how to collect and process data lawfully, **"the best interests of the child" requires a far more complicated—and comprehensive—analysis, one that involves subjective judgments and considerations beyond data protection.**[38]

Despite these challenges, addressing the issue of children's digital privacy globally offers an important opportunity for effective policymaking. There is broad agreement that protecting children from online dangers is important. But there also is growing recognition that it is essential to protect children's privacy and promote their ability to exercise increasing levels of autonomy as they mature. While it is important to protect children's data, children also have rights to expression and speech, as articulated in the United Nations' Convention on the Rights of the Child.[39] **The rapid migration of key**

aspects of children's lives online, and the global nature of the Internet, requires rethinking how children's data privacy can be addressed in a way that manages the risk of data collection and processing,[40] balances competing policy priorities across jurisdictions, and creates a digital environment that best benefits and empowers them.

The following sections consider some of the key issues challenging policymakers and companies in their efforts to protect children's digital privacy and promote their positive online experience: consent to the collection and use of data, the need to implement reliable age assurance tools, and the need to provide transparency about the collection and processing of children's data. It also considers application of a risk-based approach to digital privacy protection for children, and the challenges to be addressed to make such an approach credible and effective.

Practical Challenge: Establishing privacy floors.

Privacy floors, well-intended measures implemented to ensure that children of a designated age are protected, risk compromising the user experience and preventing older children from accessing content and activities appropriate for them. Privacy floors oftentimes practically mean that users are provided with a more limited experience (e.g., restricting or not enabling free chat on platforms designed to enable children's shared experiences). While such limitations can be appropriate for a certain segment of minor users, they may also significantly restrict the experience of users of an age when they should be able to enjoy the full user experience.

Technological solutions, such as a click-through that would enable a user to disable the privacy floor would risk allowing some children to access content not suited to them and undermine the protections the floor was designed to provide. This is especially the case as tech-savvy children often are the first to learn how to work around features that keep them from sites and activities they wish to participate in. Arrangements whereby a user's age must be determined to circumvent the privacy floor raise their own privacy concerns.

III. Consent

The question of consent—when it is required and who may provide it—is central to many laws and regulations designed to protect privacy in children's data. **Consent serves as one basis for the lawful processing of data** generally in privacy regimes, codes of conduct, guidance and best practices in countries around the world. When the data subject is a child, the issue of consent becomes more complicated.

A. Age of Consent

Protecting privacy in children's data raises questions about **when a child has reached an age at which they can provide valid consent** to the collection and processing of their data for a relevant purpose, **and when a parent or other responsible adult must provide such consent.**[41] For policymakers, establishing an age of consent in the context of privacy involves determining when a child is able to understand what consent means in a particular instance of processing and its consequences.

The age of consent in the context of data privacy varies widely across jurisdictions. This variation often reflects differences in cultural norms. In some cases, privacy law establishes the age at which children may consent;[42] in others, laws related to contract are relied on to make that determination, so that a child's ability to consent to the collection and processing of data mirrors their ability to enter into a contract.[43] Other jurisdictions take a more calibrated approach and provide that children can make certain decisions about data collection and processing at different stages in their development. Moreover, while some laws may establish an age of consent, they also may provide for circumstances when a child who otherwise may not have reached the age of consent may still be able to validly do so. In such cases, organizations must make a subjective determination about when these conditions apply. This disparity among jurisdictions reflects the reality that determining when a child is sufficiently mature and possesses the necessary awareness to provide consent to the collection and processing of data does not lend itself to bright line analysis.

The question of consent in children's data privacy is further complicated because children's awareness, maturity and need to access resources and information change and grow as they mature. The nature of the content and experiences appropriate for children evolves with their development—what is appropriate for a 15 year old is not necessarily appropriate for her eight year old brother. While this reality raises the question of whether the age at which parental consent is required should more closely track to the stages of a child's and teens' development, it is not clear how this could be practically accomplished.

Given the reach of the Internet, and children's ability and need to access platforms, information and resources from around the globe, **differences across jurisdictions and among codes of conduct with respect to the age of consent present significant compliance challenges for organizations. They also create inconsistent protections for children.** Organizations, children and families would benefit from guidance that benefits from the insight of experts, companies, policymakers and regulators about how to navigate these variations for children and their families. It could also streamline companies' efforts to obtain valid consent from children or their parents at the appropriate age, and to develop and deploy the technological tools necessary to do so.

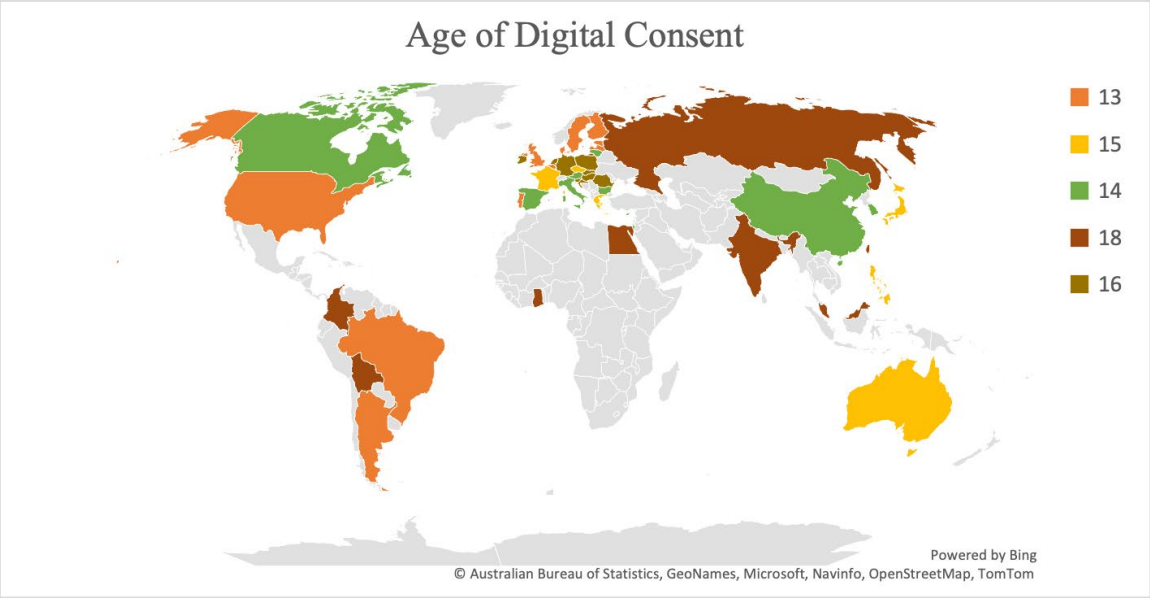

FIG 1.: Age of Digital Consent in the countries analyzed in this paper

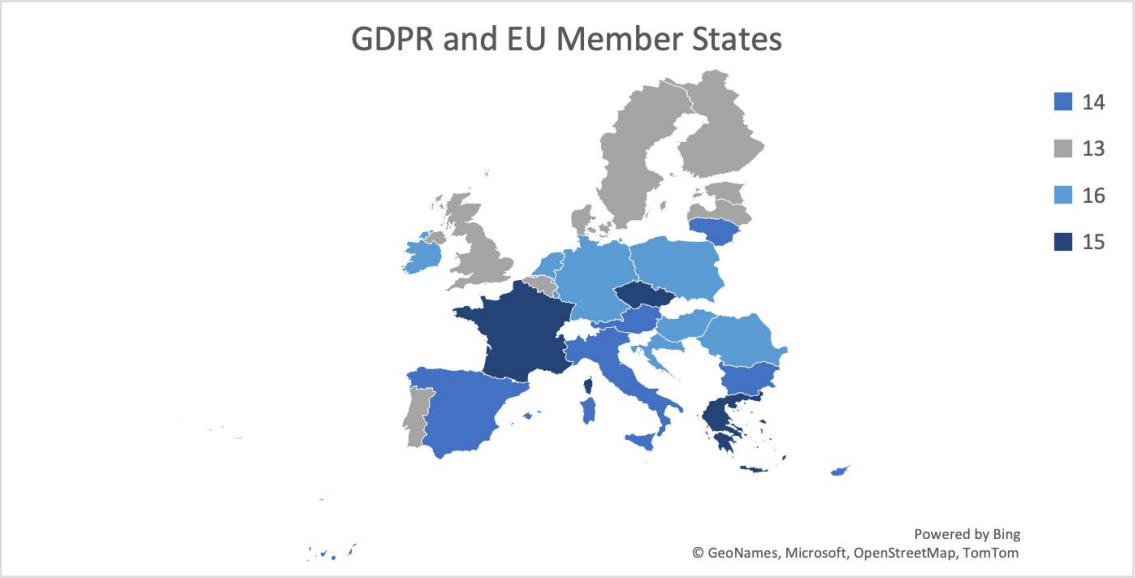

FIG 2: Age of Digital consent in the EU [where the GDPR sets it at 16] and its Member States

Practical Challenge: Complying with data regulations across multiple jurisdictions—Age of consent.

While the EU's GDPR establishes 16 as the age of consent to data collection and processing of data, the regulation enables member states to set a lower age threshold. To accommodate the variation in age requirements, companies must build and adapt offerings in different EU member states for the same online service. Many companies that make available to children valuable online content and experiences—particularly smaller companies and start-ups—do not have the resources necessary to implement age verification and consent solutions for a range of ages for a single platform, activity or service.

As an example, an online game that attracts over 1.5 million active users monthly must screen for age both to provide an appropriate experience and to seek parental consent for the collection and processing of a child's personal data when required. Because the age of consent varies and players range from age 13 to 16, the company is required to implement four different age gates in the same service.

While a company's inability to bear the costs of compliance affects its ability to access markets, it also ultimately impacts users. To defray the cost of compliance, users could be charged for access (through in-app purchasing or subscriptions). In some cases, offerings are no longer available because companies cease operations.

Practical Challenge: Obtaining consent for clinical research trials when the age of consent varies—a clinical research example.

A clinical research organization managing a study trial involving participants from Country A, Country B and Country C uses a technology tool that enables patients to create an online journal by entering daily details about their day-to-day experience over the course of the trial. Such data may include number of hours of sleep, blood glucose levels, blood pressure readings and temperature readings.

Countries A and C provide that individuals aged 16 and over can provide valid consent to participate in a clinical research trial. Country B provides that individuals can consent at age 18.

The journaling technology the researchers wish to use is offered and operates globally across many jurisdictions. In its terms of service, it provides that the technology is not intended for use by individuals under the age of 18.

As a result, trial participants in Country B can use the journaling technology. Participants in Countries A and C who are under 18 cannot.

Because the intended age is set high, the company providing the journal technology limits the risk that individuals below the age of consent will submit data through the platform and avoids potential legal exposure for collecting data from minors without valid consent in an environment where the age of consent varies across jurisdictions.

However, the clinical research organization is left to decide how to gather the daily data needed in a manner compliant with law and regulation when the age of consent for participation in a clinical research trial does not align with data collection consent requirements.

B. Who May Consent on Behalf of the Child?

Requiring the consent of a parent to the collection or processing of data when a child is not of age raises its own set of issues both for organizations and for families. For example, **parents may be unfamiliar with various technologies and data protection laws and regulations. As a result, they may not understand how parental consent works** and its consequences, so that **this cornerstone of data protection law may be limited in its effectiveness**. Moreover, laws that require parental consent may envision a nuclear family and may inadvertently discriminate against or sideline children **who**

do not live with both parents or whose parents are deceased or incapable of acting on their behalf, or do not have a child's best interests at heart, or who live in other non-nuclear family structures. They also do not reflect the experience of families where parents and children may not have their own differentiated device and where parents may not be sufficiently literate or familiar with technology to provide consent.

However, when laws, regulations and guidance broaden the definition of "parent" to include other responsible adults who may act in their place, companies are **faced with determining whether the individual who is consenting on a child's behalf appropriately may act in that capacity**. While this issue arises in many contexts—medical treatment, education, social care—it is a problem online especially because the relationship with the child is both limited and distant, so that the normal mechanisms for assessing the position of responsible adult are not available.

This question often arises in the case of pre-teens or young adolescents, who may wish to share data necessary to access information or resources designed to help them deal with questions they may not choose—or be ready—to share with their parents, such as sexual orientation, sexual abuse, gender identity, issues of body image and mental health.[44] **The availability of online resources may be particularly important to them at a critical moment in their lives that may fall below the age of consent**. In such cases, it may be necessary to **identify alternatives to traditional parental consent** in cases where no other legal basis for processing applies.

Finally, it is important to acknowledge the difficulties associated with confirming that the person providing consent is the actual parent or person who appropriately acts in that capacity. Making such a determination requires **evaluation of documentation to determine whether the individual is in fact the parent or is legitimately acting as a guardian**.[45] This is especially challenging when companies operate across a vast number of jurisdictions. Approaches to parental consent would benefit by taking this reality into account.

Practical Challenge: Verifying parental consent—proportionality and data minimization.

Companies doing business in jurisdictions that require parental consent for collection and processing of children's data must verify that the person providing consent is, in fact, a parent or in relationship with the child that would authorize them to act on their behalf. The company is also required to verify that the person providing the consent is an adult as defined by law or regulation.

Two commonly-used methods—credit card authorization and scanning of an ID document—are examples of age-verification methods that collect a significant amount of data and that may provide a level of specificity and assurance with respect to age that is disproportionate to the risk to children. While the law requires only that the company verify an individual's age and parental relationship with the child, these methods go further, providing the individual's name and other identifying information. Parents have been reported to complain that these methods are privacy-invasive, and companies assert that these methods provide a level of identification and specific certainty disproportionate to the risk of data processing in most instances.

While attempts to develop innovative age-verification solutions continue, innovators would benefit from clarity about how to determine the level of certainty and age-specificity necessary to align the risk posed to children of a specified age.

Practical Challenge: Determining age-appropriate defaults and determining which can be overridden by parental consent.

The Age-Appropriate Design Code asks operators to establish age-appropriate default settings to ensure they are operating "in the best interest of the child." Making such a determination requires careful assessment of the potential risks of data processing in the context of the capacity and interests of children and teens of various ages.

These assessments are by nature subjective and are often a function of an individual country's cultural norms, making it difficult for corporate entities to establish defaults and/or maximum settings with any degree of certainty or confidence.

Even if the operator has determined what the appropriate settings are, the question remains: up to what point can parents override those settings? Because, in some jurisdictions parents are deemed to have wide latitude to override default settings, and in others, operators are expected to set limits that can't easily be overridden, companies struggle to reconcile differences in a way that keeps them in compliance.

Greater clarity is needed about how to establish age-appropriate default settings, and what criteria should be considered when determining when they can be overridden.

C. Consent and Legitimate Interests

In some jurisdictions, consent is not the only basis for the collection and processing of data established in law.[46] **The EU GDPR[47] and the UK GDPR, for example, provide that one legal basis for processing data is a company's "legitimate interest"**. A legitimate interest may support lawful processing "except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, *in particular where the data subject is a child*" (emphasis added).[48]

Like the EU GDPR, the UK GDPR does not prohibit companies from relying on legitimate interests as the lawful basis for processing children's personal data. However, both the EU and the UK laws specifically highlight children's personal data as requiring heightened protection. UK guidance notes that if organizations rely on legitimate interests for processing children's personal data, they are responsible for protecting children from

risks that they may not fully appreciate and from consequences that they may not envisage. They must ensure children's interests are adequately protected and that appropriate safeguards are in place. Specific weight must be given to children's interests and a more compelling interest must be established.

But using legitimate interests as articulated in the EU GDPR as a possible legal basis to process children's data is arguably more difficult under the Irish Data Protection Commissioner's *Fundamentals*. The GDPR requires that organizations that wish to rely on legitimate interests as the legal basis for processing children's data must balance the necessity of an organization's legitimate interests and the right of data subjects.[49] However, using the legitimate interest basis for processing children's data, while not impossible, is actively discouraged in Fundamental 3, which imposes a zero-tolerance approach to any encroachment on a child's best interests. Fundamental 3 states that "the child's interests or fundamental rights should always take precedence over the rights and interests of an organization which is processing children's personal data for commercial purposes". Also, the Fundamentals notes that "in circumstances where there is any level of interference with the best interests of the child, this legal basis will not be available for the processing of children's personal data".[50]

Enabling companies to rely on legitimate interests as a legal basis for processing children's data could benefit both companies and families. Eliminating the need to approach parents in each instance of processing would relieve parents of the need to constantly reiterate consent to basic processing they have already agreed to. It would allow companies to more readily engage in practices that enhance children's experiences and their safety.

Practical Challenge: Variations in Consent Requirements, and the Problem of Cookies.

The age at which consent to the collection and processing of data is valid varies across jurisdictions. The US Child Online Privacy Protection Act (COPPA), for example, sets the age of consent at 13. Across the EU, that age varies from 13-16. In other jurisdictions, individuals may be able to provide valid consent until they are 18.

The method by which a company can obtain valid consent also varies depending on the applicable law. COPPA requires companies to implement a neutral age gate for a service targeting users of mixed ages that does not signal to the user at what age they are able to access different features and functionality. Therefore, a tick box stating "I am 13 years old" does not meet the US' COPPA requirements. In the EU, developers must prove that consent is valid, that it is informed and granular and that they have methods in place to allow parents to exercise their rights in relation to children. This may require parent dashboards or a parent portal to enable management of consent and revocation. In some cases, jurisdictions may ask for official identification to verify age and to assess whether the individual is, in fact the child's parent.

These age screening requirements, and the mechanisms implemented to meet them, are further complicated when laws and regulations in addition to children's privacy law apply. The EU ePrivacy Directive, for example, imposes additional obligations on companies, requiring consent from the user for the use of certain cookies.

It is not clear how such consent can be validly obtained in the case of children, who will likely simply click on banner notices to continue. Companies lack clarity about how to reconcile competing legal requirements and to implement the measures necessary to comply in practice. Smaller companies—some of which may provide valuable services, including educational experiences and support for children—may not be sufficiently resourced to resolve and address these conflicting obligations.

Authenticating users, securing platforms and networks, and keeping predators off sites intended for children are important examples of activities that are essential to a company's ability to do business and relevant to protecting children from harm. Clarity about how and when children's data may be used to further these goals will be important. As a general matter, **companies would benefit from the guidance of data protection authorities and other appropriate bodies about what interests and risks a company should evaluate when determining whether data may be processed to further its legitimate interests**. Ideally, such guidance would benefit from consultation with companies, families and other knowledgeable stakeholders.

IV. Age Assurance

A. The Role of Age Assurance in Protecting Children[51]

New laws, guidance and codes of conduct related to protecting children increasingly make it necessary for websites and apps to verify the age of users. The UK Age Appropriate Design Code requires that companies establish age with a level of certainty that is appropriate to the risks data processing poses for children. In December 2021, the French government threatened to block pornography sites unless the owners implemented more thorough age verification.[52] Policymakers in the US have renewed discussions about updating COPPA, the primary American law designed to protect Internet users under age 13.

Age assurance tools can be called upon to ensure that companies do not collect data from children under the legal age, depending on the jurisdiction, without parental consent.[53] **They also can help companies be more certain about the age or age range of the user to help them better comply with requirements** in law and guidance designed to protect children online. Age assurance mechanisms can require users to demonstrate that they are of an appropriate age or age range to access content and aid in blocking their access to inappropriate material or activities. It also can be used to flag adult users and keep them out of online environments designed for children. While the following discussion highlights the challenges inherent in providing age assurance, CIPL's forthcoming paper will highlight existing and anticipated solutions.

Practical Challenge: Improve the efficacy of self-declaration and improve and reduce the incidence of false age information.

Self-declaration as a method of age verification is widely recognized as not as reliable as the supervisory authorities would like. Companies seek non-privacy invasive measures that would improve its effectiveness.

Can enhancing the experience of users below the age of digital consent reduce underage children's interest in services that are not meant for them, and so limit the incentive to lie in the age gate?

Can simplifying and reducing the friction parents experience in the verified parental consent process reduce parents' incentives to circumvent the consent mechanisms and motivate greater parental involvement and compliance? Would the creation of a privacy-preserving database of pre-verified parents serve as an easier, more reliable path to valid parental consent?

B. Privacy Issues Raised by Age Assurance Solutions

While age assurance tools attempt to address the important problem of keeping children safe online, **most methods of verifying age create their own set of privacy issues**. They also suffer from a lack of consensus among regulators globally as to whether they are effective, appropriate and support compliance with data protection law. Simply asking a user to verify that they are of the appropriate age, by checking a box or providing proof of age using, for example, a credit card or government-issued identification provides little assurance that the assertion is true. Young people who are of the age of consent (and in some cases their parents) may not have official identification documents so that, without other methods, they would be excluded from access to age-appropriate online materials or activities. Enterprising children, who are often more sophisticated about online transactions than their parents, quickly understand how such age verification works and can easily check an appropriate box, falsify an ID, or use their parents' credit card to access content without their parent's knowledge.

More rigorous methods which offer greater assurances that an online user is of an appropriate age to provide valid consent to the collection and processing of data, or to access certain content or platforms often raise concerns about the collection of the large amounts or type of data needed to establish an online user's age. While access to reliable data about a child's date of birth, family, school and online activity could verify a child's age with a high level of certainty, the practical difficulties involved in accessing reliable data and the privacy implications of gathering, and potentially storing such data, are

clear. These concerns may be exacerbated when the data collected for age verification is based on biometric data. This data may include 1) data such as facial image or voice imprint that uniquely identifies an individual and 2) data such as keystroke dynamics or facial dimensions, that enables assessment to determine age, without identifying or seeking to identify the individual.

Identifying a solution to age assurance will require balancing the need for accurate, verifiable age-gating with concerns for children's privacy. Striking this balance will require understanding the risks that use of data for verification may raise and taking steps to mitigate them. It also suggests a need for proportionality—determining what level of age certainty is needed under various circumstances and tailoring the rigorousness of the verification—and the amount of data collected—accordingly.[54] [55] In some cases layered age assurance techniques may offer solutions, by requiring age assessment be more than one process or test.[56] Layered age assurance could offer multiple levels of authentication, depending on the activity, a young user may want to participate in the content or experience they may wish to access.[57] It could also make it possible to adapt age assurance techniques over the course of a user's relationship with the digital site or service.[58]

Finally, the possibility of long-term storage of data about children and its potential sharing with third parties or use for secondary purposes, such as advertising, raises legitimate concerns about profiling of children and creating stores of data that will attach to them into adulthood. To avoid these, some providers use the results of age verification in real time—on a one-time basis—and immediately dispose of them to avoid storing them at all.[59] However, a provider may need to retain information in some instances. For example, it may retain data associated with age verification awaiting the outcome of an appeals process if the user is denied access to, or removed from, the service based on the age verification process. Similarly, if an age assurance process requires the user's date of birth, a service may need to retain that data so that it can provide age-appropriate settings that evolve based on the users' ages and evolving capacity. Given the challenges involved, practical guidance from regulators, developed in consultation with industry and other stakeholders about the processing and storage of data collected for this purpose, would provide developers with a reliable foundation for solutions that allow for innovation, companies with greater certainty about their obligations when deploying age assurance methods, and parents and children with tools that work.

Practical Challenge: Implementing effective age declaration and verifying the age of users in compliance with the UK Age Appropriate Design Code.

The UK Age Appropriate Design Code requires that operators know the ages of their users to enable them to apply appropriate safeguards. Because children and teens in most cases do not hold hard ID (e.g., a driver's license), currently the only workable way to obtain a user's age is to ask them to self-declare in a neutral age gate. However, data protection authorities suggest that self-declaration is not a sufficiently reliable age verification method. Companies would benefit from clarity about how to implement effective age verification, particularly in the case of teens.

C. Artificial Intelligence for Age Assurance

Age assurance technologies that rely on artificial intelligence (e.g., those that rely on analysis of online activity or face detection) are designed to complement current techniques. These technologies obviate the need for a user to provide an official identification card (which many children do not have) or for sites to obtain the consent of parents. They also prevent children from working around existing age assurance tools, by obtaining their parents' credit cards or IDs and providing them to the site. The technology can allow for real time assessment of a user's age, and can be designed to provide an estimation, rather than confirm a precise age, when the risk of access to an activity or content does not call for exact age verification.

1. Data Privacy Risks

While AI promises to enhance age assessment and improve consent, it also requires data to learn and improve. Depending on the application, the data collected to train AI for age assessment may be sensitive. It may also include biometric data—such as fingerprints, voiceprints, scans of a hand, facial geometry recognition and iris or retina recognition.[60] AI raises concerns about processing training data for purposes other than age assurance, including to create profiles that may be further used when children enter adulthood.

AI also challenges organizations' ability to apply traditional fair information practice principles such as openness, consent, purpose specification, use limitation and accountability. Providing transparency and explaining how data is processed in AI is notoriously difficult. AI technology is complex and dynamic, and explaining to lay users how data is processed. and the purposes to which it will be used. is challenging at best. Therefore, obtaining informed consent for data collection and use of AI, when required, is challenging as well. Law, regulation and codes of best practice in many cases limit

data collection to that necessary to accomplish a stated purpose. **These requirements exist in tension with the need to introduce large quantities of new data to AI systems to train and improve its accuracy and enable it to accomplish its stated purpose.**[61]

2. Accuracy and Oversight Risks

While AI can provide powerful solutions, it is not 100% accurate and is not a perfect tool. AI must be trained and improved using new data introduced to the system, and the quality of the data entered for this purpose directly affects the quality of the results of AI. In some cases, if appropriate safeguards have not been implemented, the results of AI can be unfair, incorrect or discriminatory for children, raising concerns similar to those raised by data processing generally: **if not properly designed and monitored, AI could limit children's access to online activities and content, and impede their ability to take advantage of online opportunities that help them grow and develop or fail to protect children** from identified harms.

At the same time, sometimes having more data to ensure that AI is properly trained can mitigate these concerns. But collecting and processing that data may raise privacy issues. **Resolving discriminatory bias, for example, could require using more data collected from a vulnerable group, including sensitive data**. Organizations are faced with evaluating the varies trade-offs.

Oversight will be necessary if AI is to serve as a reliable, credible and fair age-verification tool.[62] At the same time, better education about how AI works, its role in protecting children and the way companies mitigate the risks it may raise to children, will be essential if it is to be relied upon as a trusted age assessment tool.

V. Profiling for Targeting to Children

The use of online profiling to target advertising and content to children brings together concerns about children's well-being and issues of children's privacy.

Children's advocates cite children's exposure to an extraordinary volume of advertising online. They note that children, who may not have the cognitive capacity to understand the intent of advertisements, are particularly susceptible to manipulation.[63] From a privacy perspective, the use of profiling to target children's advertising raises concerns about the amount and nature of data used to create those profiles, and the possibility that they will be used by third parties for other purposes.

Profiles created for targeted advertising can be created at varying levels of detail. Understanding an online user's age range and general geographic location can, by itself, provide the necessary information to know whether that person is of age and living in a jurisdiction where they can legally order delivery of alcoholic beverages.[64] Other profiles involve creation of highly specific descriptions of a single individual.

Used another way, however, profiles can also benefit children by helping ensure that children are offered content that is appropriate for their age, level of development and interests. They can help to keep them away from content, activities or products not suited to them.[65] These potential positive uses raise the question of whether creating profiles to target children—either for advertising or to direct appropriate content to them—can be carried out in a way that is not harmful and respects their privacy. The *UK ICO's Age Appropriate Design Code*, Provision 5, addresses this question. It states that children's personal data should not be used in ways that are detrimental to their wellbeing, and includes a section on marketing and behavioral advertising that highlights:

- physical, mental or moral harm to children;
- exploiting children's credulity and applying pressure;
- direct exhortation of children and undermining parental authority; and
- promotions.

The *Code* states that if a company "profile[s] children (using their personal data) to suggest content to them, it must put in place measures to make sure that children are not served content detrimental to their physical or mental health or wellbeing, taking into account their age". Provision 12 on profiling also states that under the code, any user self-declared as under 18 should have behavioral advertising turned off by default.[66] However, absent such self-declaration, determining whether a teenager is 18 and not 17 requires a robust age assurance system.[67]

While the *Code* provides criteria for companies to consider when making decisions about direct marketing and behavioral advertising to children, the Irish Data Protection Commission's *Fundamentals* document suggests a stricter standard: data controllers should not engage in direct marketing activity unless they can demonstrate that it "positively promotes the best interests of the child".[68] **Such beneficial marketing might inform the child about the existence of counseling or support services, health and social resources, education opportunities and tools, and organizations that provide advocacy and representation for young people**.

The Office of the Privacy Commissioner of Canada also has acknowledged the difficulties in obtaining meaningful consent for online behavioral advertising from children and has indicated that organizations should avoid tracking children and tracking on websites aimed at children.[69]

The European Parliament's draft of the DSA highlights one of the tensions inherent in attempting to resolve the issue of minimizing the collection of children's data while also putting in place robust age verification. The DSA prohibits targeted marketing to children if the platform is "aware with reasonable certainty" that the person receiving the service is a minor. It also states that this requirement "shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor". Thus, on the one hand, the proposed DSA imposes limitations on targeted advertisements to children while also not requiring additional data collection for age verification, raising a compliance challenge around the question of what criteria would, in fact, establish "awareness with reasonable certainty" whether someone is a minor and whether the DSA, despite its wording, imposes a de facto age verification requirement.

Moreover, the EU's GDPR and other privacy laws also require controllers to minimize the amount of data they collect and process, limiting themselves to what is directly relevant and necessary to accomplish a specified purpose. How a provision of this kind would interact with a potential de facto age-verification requirement under the DSA deserves further clarification.

VI. Providing Transparency About the Use of Children's Data

Providing data subjects with information about a company's data practices is a critical element of data protection regimes and at the forefront of regulatory enforcement strategies. Openness about the collection and processing of data is one of the principles of fair information practices that form the basis for data protection and privacy laws, regulations and guidance around the world.

What companies can do to enhance transparency about the collection and processing of children's data represents an aspect of the broader question about how to effect transparency about data use generally. As data collection has become more ubiquitous and seamless, **and as processing becomes more complex and increasingly occurs in real time, providing data subjects of any age with information about data collection and processing has become more difficult.** Drafting a clear, easy-to-understand privacy notice that complies with legal requirements and making it available in a form and at a time when it is useful to the user is widely recognized as a difficult undertaking. In many cases, individuals simply want the information they need to get to the resource or platform they need to access, and **privacy notices are perceived as an impediment.**

Despite these challenges, transparency remains an important element of data protection law, regulation, enforcement and guidance, particularly with respect to children's data. The EU's GDPR[70] contains more specific provisions about the information that companies must provide to data subjects when processing their personal data.[71] Article 12 of the EU's GDPR requires that children are provided with this information in a way in which they can access and understand it.[72] The UK's *Age Appropriate Design Code* sets out specific requirements with respect to how companies should provide transparency about the collection and use of children's data in compliance with the UK GDPR.[73] It also makes detailed recommendations about how transparency should be provided for children within various age ranges.[74] Other existing and emerging data protection laws require operators to be transparent about the collection and processing of data about children.[75]

Under the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, consent is valid only if it is reasonable to expect that the individual would

understand the nature, purpose and consequences of the collection, use or disclosure to which they are consenting. This requires organizations to carefully consider how they explain their privacy practices to ensure that meaningful consent is obtained.[76]

Determining how transparency can be provided effectively so that it serves children and their families will be important in this context. Providing information that is useful for children raises challenges related to their ability to understand, at various ages, the information that is being conveyed to them and its implications. Simply getting and keeping children's attention long enough to take in the information being conveyed is its own challenge. Because parents and caregivers—many of whom are not necessarily knowledgeable about the Internet and data use—are often required to provide consent to the collection and processing of children's data, providing them with clear, understandable information that can form the basis for that consent presents its own set of challenges.

Providing transparency that serves the needs of children and their families requires an understanding of what information they want and need, and about when and how it is best to provide it. Technology and innovative interfaces may provide opportunities to offer information to children and their parents at critical points during their engagement with a site or service. Because both children and their families require information about data collection and use, organizations will need to consider how to communicate effectively to both.

Efforts at transparency may also be served when designed in the context of initiatives to promote greater data and online literacy generally for children and their families. Resources specifically designed to enhance transparency for children may also offer the additional benefit of empowering them to make decisions appropriate to their age and maturity and help them understand the choices parents or guardians make for them.

As new approaches to protecting children's data privacy and fostering better literacy about data protection issues are considered, it will be important to learn from existing efforts to educate children and parents about online safety and privacy.

Practical Challenge: Writing age-appropriate, understandable notices for children.

Companies required to post age-appropriate privacy policies face the dual challenge of developing language that communicates to young people and implementing technical measures to make those notices available to the right child at the right time. Writing privacy notices that are clear, comprehensive and understandable is difficult when they are intended for adults. Writing them for children involves additional challenges.

The UK's Age Appropriate Design Code outlines age ranges and developmental stages for this purpose. However, understanding what an 8-year-old will understand versus what is helpful to a 15-year-old is a skill most businesses—particularly smaller companies or start-ups—do not have. Technically implementing the notices in a way that makes them accessible to the right child at the appropriate time is a challenge, but particularly so when they must be made available on small screens and in applications like games and AR and VR experiences.

Practical Challenge: Implementing age-appropriate disclosure requirements for children across different age groups.

Companies in many instances are required by law, regulation or statutory code to post privacy policies that are transparent, meaning that they should be understandable and suited to a child's age and capacity. Privacy policies must meet the needs of users who range from young children to teenagers.

These transparency requirements across jurisdictions require organizations to make available to minors simplified, concise and clear privacy policy disclosures. For organizations whose goods, services and platforms are child-oriented, it may be necessary to post a child-friendly version of the privacy policy over a policy intended for parents and adults. This challenge is further heightened when operators make their goods, services and platforms available in many jurisdictions whose disclosure regulations may vary. This is further complicated when the company offers an extensive array of platforms, tools and services.

Efforts to accurately communicate several different age-specific versions of a policy for single online service exposes companies to increased legal risk and raises questions about which policy is required for which child and which jurisdiction, and whether users at certain ages should be directed to a policy of greater complexity. The potential for inconsistencies or perceived inconsistencies between various articulations of the same policies may create consumer confusion and exposes companies to increased legal risk and user complaints. Moreover, determining which privacy notice should be made available to a user requires that companies understand a user's age bracket and jurisdiction to match them to the appropriate policy, raising additional privacy concerns.

VII. A Risk-based Approach to Children's Data Privacy

A risk-based approach to the protections of children's data—one which involves assessing the risks and benefits to children[77] that collecting and processing their data may raise and taking steps to mitigate the risks and preserve the benefits—has been suggested as a path toward effective governance for children's privacy. Such an approach is reflected in the ICO's *Age-Appropriate Design Code*, which specifically requires companies to carry out data protection impact assessments to assess and mitigate the risks to the rights and freedoms of children raised by data processing. The Irish Data Protection Commissioner's *Fundamentals* also advises companies to conduct data protection impact assessments (DPIAs) that considers the best interests of the child.

Adopting a risk-based approach to addressing privacy in children's data would reflect developments in data privacy generally. In addition to the guidance documents noted here, emerging law, regulation and policy increasingly include requirements that companies be accountable for their data practices and the steps they take to protect individuals from the risk of harm data collection and processing may pose. Data governance that relies, at least in part, on risk assessment and mitigation is a key element of, for example, the GDPR, the Asia Pacific Economic Cooperation Privacy Framework, Canadian privacy legislation, Colombia's Data Privacy Law and related Decrees, and proposals for a comprehensive privacy law in the United States.

A risk-based approach could shift the burden of protecting children's data away from parents (via consent) to companies that will use risk assessment and tailored mitigations to address the potential harm to which specific data collection and processing activities might expose children.[78] However, a risk-based approach that is workable and results in an appropriate balancing of the benefits and risks of use of children's data will need to be thoughtfully designed and implemented.

Because issues of children's privacy also implicate questions of children's safety, their right to participate fully online, and the right of their parents to supervise their online activity (to an appropriate extent), assessing the risks that processing children's data

poses is a complex undertaking. **For such risk assessments to be credible in the eyes of the public and regulators, it will be important to provide clear regulatory guidance and articulation of the relevant criteria** companies will need to meet when implementing a risk-based approach.

Indeed, as with DPIAs generally, where DPIAs play a role in evaluating risks to children, companies will need guidance about the risks of harms—particularly those specific to children—they are to measure, and what competing interests they are to evaluate and balance. It may be useful to look to current company experiences when carrying out DPIAs to comply with data protection laws generally. What challenges do companies confront when conducting a DPIA, and what can be learned from these processes as currently deployed? What risks to individuals are measured? How are benefits assessed and weighed against risks? **Understanding how a risk-based approach currently works in practice could provide insights when attempting to determine the risks specific to children DPIAs should take into consideration.** They may also help identify how concerns beyond privacy—children's rights, their need for information, and their best interests—might be incorporated into a DPIA, if it is appropriate to do so. As DPIAs may not be the only assessment a company may be obligated to carry out when releasing a new technology (for example, the EU Artificial Intelligence Act (AIA) requires companies to conduct a conformity assessment prior to the release of some AI systems in the market; Article 26 of the EU Digital Services Act requires that very large online platforms identify, analyse and assess at least once a year any significant systemic risks stemming from the functioning and use made of their services), practical guidance from regulators, developed in consultation with companies and other relevant stakeholders and preferably with a high degree of global consistency about what criteria should be evaluated during the DPIA process would help companies identify, assess and mitigate perceived risks.[79]

Effective oversight also will be key to the credibility of the risk-based approach. Companies will need to understand what their obligations are with respect to carrying out data protection impact assessments, memorializing and being able to demonstrate their assessment process and decisions, and implementing their risk mitigation strategies. **They will also need to understand the criteria by which data protection authorities will evaluate their internal risk assessment processes**, and how data protection authorities will take them into account when investigating instances of privacy violations or failures.

Finally, because of the reach of the Internet, **cross-border recognition of such an approach will be important to streamline global compliance**. International guidance and codes of conduct that address requirements and criteria for compliance could provide the basis for meaningful and credible compliance, and supervisory oversight.

VIII. Conclusion

While the right of children to a positive online experience is beyond question, designing a regulatory approach that protects the privacy of their data and fosters an environment in which they can grow, learn, socialize and express themselves, is a complex undertaking.

Policymakers, regulators and companies seeking to protect children's data privacy find themselves faced with having to reconcile competing concerns about how to keep children out of harm's way, make available to them the resources and information they need, and respect their growing maturity and evolving capacities as they move toward adulthood. The measures necessary to comply with children's data protection obligations often raise their own privacy risks or are prohibited by other aspects of law. Compliance with requirements of data protection laws is further complicated by the need to reconcile them with laws and regulations designed to promote children's safety and well-being in other aspects of their online experience. Increasingly, organizations are required to keep in mind the need to further the best interests of the child and to consider the benefits and risks to children as they make decisions about data collection, processing and storage. Such considerations do not lend themselves to bright line analysis or easy answers, particularly because children's capacity to understand and make wise decisions about data use grows and changes as they mature.

The global reach of the Internet further complicates this challenge. Companies doing business across jurisdictions must comply with country laws whose requirements often diverge and conflict. **Because society's attitudes about privacy and about what measures are necessary to keep children safe are culturally driven, they resist calls for harmonization or suggestions to depart from existing local norms.**

The enormity of this challenge calls for a deeper understanding of the issues and identification of possible reasonable measures that might streamline the regulatory burden for companies while providing consistent, predictable protections for children. The Centre for Information Policy Leadership looks forward to convening experts, policymakers, regulators and companies to engage in productive dialog and consensus building that will promote effective data protection and the safe, constructive online experience children deserve.

In Policy Paper II, CIPL will highlight existing and potential solutions and new innovations designed to provide protections for data while fostering a positive experience for children.

Appendix One: Survey of Laws and Regulations in Key Jurisdictions

Argentina

The Personal Data Protection Law[80] (PDPL) governs privacy in Argentina and establishes the principles and rules that apply to the protection of personal data. Several decrees, among them Decree 1558 of 2001,[81] set forth detailed rules regarding the PDPL's implementation. The National Criminal Code, as amended by the Act and Law No. 26.388 of 2008, sanctions violations related to data confidentiality with fines and imprisonment.[82]

The PDPL does not expressly address data pertaining to minors and does not specify the criteria by which a minor's consent is considered valid. However, the National Civil and Commercial Code[83] provides that minors (children under 18 years old) lack the capacity to exercise their rights.

The Argentine data protection authority (AAIP) has issued detailed guidance about implementation and compliance with the PDPL in its 'Guiding criteria and indicators of best practices in the application of the Act' (the AAIP Criteria).[84] This guidance corresponds to the Commercial Code's criteria. It distinguishes between minors under and over 13 years of age, and it establishes the presumption that while children under 13 cannot perform "voluntary rightful acts," children over 13 can if they are sufficiently mature. The Commercial Code also provides that when minors enter into contracts of small value, those contracts are presumed to be entered into by their parents.

The AAIP Criteria provide that whether minors may give informed consent for the processing of their personal data depends on their aptitude and level of development. If a minor does not have sufficient capacity to provide informed consent, consent must be obtained from a parent or guardian. In such cases, the person or entity obtaining consent must make reasonable efforts to verify that it was provided by the holder of parental responsibility.

Australia

In Australia the Privacy Act 1988 (No. 119, 1988)[85] (the Privacy Act) provides for the protection of an individual's personal data. It incorporates the 13 Australian Privacy Principles, which align with fair information practices as articulated in the Organization for Economic Cooperation and Development's privacy guidelines.[86]

The Privacy Act governs how personal data is handled by organizations across a range of sectors, however, it includes no specific provisions addressing children's personal data. Instead, children's privacy in Australia is governed by a mix of general privacy legislation, online safety regulation and legislation that does not address privacy but rather imposes obligations related to confidentiality and record handling.

The Privacy Act provides that, for consent to be valid, an individual must possess the requisite capacity.[87] It does not specify whether children have the capacity to consent, nor does it specify an age in which an individual can make their own privacy decision.

While the age of majority in Australia is 18, guidance released by the Office of the Australian Information Commissioner notes that, as a general principle, children under 18 only have the capacity to consent when they are mature enough to understand what is being proposed. An organization or agency handling the personal data of an individual under the age of 18 must, therefore, decide on a case-by-case basis whether the individual has the capacity to consent. If such a case-by-case review is not practical, the OAIC advises that, with some exceptions, persons 15 and over have the capacity to consent. Where they lack sufficient maturity, however, the OAIC guidance states that it may be appropriate for a parent or guardian to consent on their behalf.[88]

Australian laws and regulations do not contain provisions that specifically apply to children's privacy in the context of education. The Privacy Act governs private sector education facilities; these institutions must comply with the Australian Privacy Principles when handling personal data about the children. Public sector education institutions must comply with laws that govern the state and territory governments' collection and processing of personal data.

Bolivia

Bolivia has not enacted a general data protection law. However, data protection is provided for through laws that apply across industry sectors and activities. For example, the Telecommunications Law No. 164 of 8 August 2011[89] and its related regulation, the Supreme Decree No. 1391, establish a general regulatory framework for personal data. The General Consumer Rights Law 2013[90] establishes that vendors must adopt appropriate mechanisms to guarantee the confidentiality of their customers' data. Similarly, Supreme Decree No. 28168/2005[91] establishes that any person may request that their data be updated, supplemented, corrected or deleted.

There is no law governing children's data specifically, however, The Code of the Boy, Girl and Adolescent provides that, as a general matter and with some exceptions, persons under the age of 18 are unable to give consent.[92]

Brazil

Brazil's General Personal Data Protection Law[93] (LGPD) governs the activities of data controllers and processors and sets forth requirements for processing personal data. The LGPD establishes, for example, requirements for data protection impact assessments and the appointment of data protections officers. It also sets forth the conditions for data transfers and data breach notification.

The LGPD includes specific provisions related to children's data. Article 14 (1) states that children's and teenagers' data should be processed in accordance with the law and in a manner that takes into account their best interests.[94] According to Brazil's Child and Adolescent Statute, a child is any person up to 12 years of age, and an adolescent is any person between 13 and 18 years of age.[95]

The LGPD requires parental consent for all processing activities involving children's data.[96] It further requires that all reasonable efforts be made to verify that consent has been provided by the parent responsible for the child, bearing in mind the technologies available to support consent.[97]

Children's data may be collected without parental consent, however, in certain circumstances, i.e., when collection is necessary to contact the parent or legal guardian or for the child's protection. In such cases, it may be used only once and may not be stored. In no circumstances may the child's data be passed on to a third party without parental consent.[98]

The LGPD also states that data controllers may not condition the child's participation in games, internet applications or other activities on their providing personal data beyond what is strictly necessary for the activity.[99]

Finally, the LGPD includes detailed requirements related to transparency, and sets out how information about processing of children's data should be made available. It states that such information is to be provided "in a simple, clear and accessible manner," taking into consideration the user's maturity and stage of physical and intellectual development. It must also make use of audio-visual resources when appropriate and "provide the necessary information to the parent or legal guardian that is appropriate to the child's understanding".[100]

Canada

Canada has an established and extensive privacy law framework, including over 35 federal, provincial and territorial privacy statutes governing the personal information practices of organizations in the public, private and health sectors. While there is no legislation in Canada that specifically addresses the protection of personal information of children, Canadian privacy laws apply to the collection, use, disclosure and other processing of a child's personal information. Four statutes in Canada govern privacy in the private sector. These include the federal Personal Information Protection and Electronic Documents Act 2000 (PIPEDA), the British Columbia Personal Information Protection Act,[101] Alberta's Personal Information Protection Act[102] and Quebec's Act respecting the Protection of Personal Information in the Privacy Sector.[103]

In general, the personal information of minors is considered sensitive under Canadian privacy statutes.[104] Express consent is generally required for the collection, use, disclosure and other processing of sensitive personal information. Because children's personal information is considered sensitive, the provisions of Canada's privacy statue will be more strictly applied.

While there is no prescribed age of consent under existing privacy legislation, amendments to the Quebec Private Sector Act, which comes into effect in 2023, prohibits the collection of personal data from a minor under the age of 14 years without the consent of the person having parental authority, unless collecting the data is clearly for the minor's benefit.[105]

China

China's comprehensive data privacy law, The Personal Information Protection Law (PIPL)[106] came into effect on 1 November 2021. The PIPL governs the processing of personal data by entities or individuals within China. Two additional laws relevant to data protection in China are the Cybersecurity Law and the Data Security Law. The Civil Code provides for the right to privacy and the protection of personal data.

The Personal Information Protection Law

PIPL Article 28 defines sensitive personal data as data that, once leaked or illegally used, might easily cause harm to the dignity of natural persons and grave harm to personal or property security. Sensitive data includes the personal data of minors under the age of 14. PIPL Article 31 requires personal data handlers to provide specific notice when processing personal data about minors and to obtain the consent of the parent or other guardian of the minor.

Cyber Protection of Children's Personal Information

China's Provisions on Cyber Protection of Children's Personal Information (Provisions) became effective in October 2019. These comprise the first rules focusing on the protection of children's personal data in China.

The Provisions define children as minors under 14 years old.[107] They govern activities relating to the collection, storage, use, transfer and disclosure of children's personal data via networks in China. The Provisions do not apply to such activities conducted outside of China, nor to similar activities conducted offline.

The Provisions set up a higher standard of consent than the Cybersecurity Law of China. Network operators who wish to obtain informed consent from a parent or guardian must provide a mechanism whereby consent can be declined. It also must specifically inform guardians of:

- the purpose, means and scope of collection, storage, use, transfer and disclosure of children's personal data;
- the storage location of children's personal data, retention period and how the relevant data will be handled after expiration of the retention period;
- the safeguard measures protecting children's personal data;

- the consequences of rejection by a parent or guardian;
- the channels and means of filing or reporting complaints; and
- how to correct and delete children's personal data.

The Provisions also require a network operator to restrict internal access to children's personal data. Specifically, personnel are prohibited from accessing children's personal data unless authorized by a designated staff person inside the organization.

Network operators who wish to transfer children's data to a third-party processor must conduct a security assessment and establish with the third party the necessary contractual requirements. Data processors are forbidden to subcontract its children's data processing services. The third-party data processor is required to assist the network operator in complying with the parent or guardian's request to delete a child's data after termination of service.

Similarly, when children's personal data is to be transferred to a third party, the network operator is required to conduct a security assessment of the third party.

Colombia

Privacy in Colombia is governed by two laws. The first of these is Statutory Law 1266 of 2008 (December 31)[108] which Establishes General Provisions of Habeas Data and Regulates the Management of Information Contained in Personal Databases, specifically Financial, Credit, Commercial and of Services and Derived from Third Countries and Other Provisions.

The second, Statutory Law 1581 of 2012 (October 17)[109] Which Issues General Provisions for the Protection of Personal Data (the Data Protection Law) seeks to develop as a constitutional right, the ability of individuals to "know, update and correct data" collected and maintained about them.

With respect to data privacy, children and teenagers (individuals under 18 years old) enjoy special constitutional protection,[110] and their personal data must be processed in accordance with their applicable rights. According to Article 7 of the Data Protection Law the personal data of individuals under 18 may not be processed unless it is 'public nature' data.[111]

However, it is important to note that Colombia's Decree 1377 of 2013[112] provides for exceptions, allowing the data of minors to be processed when necessary for the protection of the minor's fundamental rights. The Decree specifies requirements for the processing of personal data of children and teenagers. Such processing must:

- respect their interests; and
- be carried out in a way that guarantees their fundamental rights.

The informed, expressed consent of a parent or guardian must be obtained before processing minors' personal data.

Egypt

The Law on Data Protection[113] (Data Protection Law) establishes the standards and rules designed to protect the rights of individuals in Egypt in their personal data.

Article 1 of the Data Protection Law includes data pertaining to children[114] in the definition of "sensitive data".[115] The Child Law No. 12 of 1996 defines a child as any individual under the age of 18.

Article 12 of the Data Protection Law further provides that the transfer, collection, storage or processing of children's data requires the consent of a guardian. It also states that a child's participation in an online game or other activity must not depend on their providing more data than is necessary to enable their participation.

European Union

Data protection in the EU is governed by two laws: the General Data Protection Regulation (GPDR)[116] and the Directive on Privacy and Electronic Communications (ePrivacy Directive).[117] Protection of children's data is addressed in the GDPR.

The GDPR provides that personal data be processed in accordance with principles of fair information practices. Article 6 of the GDPR sets out the bases for the lawful processing of data. Among these bases is the consent of the data subject.

The GDPR includes rules governing consent to data processing when "information society services"[118] are offered directly to children and consent is the appropriate legal basis for processing data. If the child is between the ages of 13 and 16, depending on the Member State, data controllers must obtain the consent of the "holder of parental responsibility" if processing is to be considered lawful.[119] Data controllers must also make reasonable efforts to verify that the holder of parental responsibility has consented.[120]

Information about matters related to the collection and processing of data must be provided to a child and must be easily understandable and provided in clear and plain language.[121]

The GDPR provides that data subjects can demand that controllers delete personal data pertaining to them when certain conditions are met. Deletion may be demanded when personal data has been collected in relation to the offer of information society services directly to a child and the child consented, but they were not fully aware of the risks raised by the processing at the time. The GDPR provides that the right may be exercised even if the data subject is no longer a child.

The GDPR calls upon EU Member States, their data protection authorities, the European Data Protection Board and the European Commission to encourage relevant organizations and parties to develop codes of conduct that address how the requirements of the GDPR should be met. One example of such codes noted are those regarding "information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained".[122] Nationally accredited bodies may be authorized to oversee compliance with the codes of conduct.[123] [124]

Variations in Certain Requirements

The GDPR applies directly in EU Member States and generally requires no implementing legislation. However, it provides that Member States law may vary somewhat from its provisions in some instances. One of these is the age of consent. The GDPR provides that a parent or legal guardian must consent to a company's processing of personal data for children under 16, and to as low as 13 years of age.[125] But it also provides that a Member State may set its age of consent lower than 16.[126] As a result, the age of consent varies across the EU. Various Member States have set the age at 13, 14 or 15.[127]

Variations also exist with respect to the issue of age verification. Portugal requires that a company obtain permission from a legal guardian through a secure means of authentication. Germany[128] and Romania, however, require only that data controllers make reasonable efforts to verify that the person with parental authority has consented on behalf of the child. Significantly, guidance about how this determination should be made has not been provided in either of these countries.[129]

Ghana

Ghana's Data Protection Act[130] establishes a Data Protection Commission (DPC), charged with protecting individuals' privacy and personal data. The DPC regulates, among other matters, the processing of personal data, the rights of data subjects and the processing of personal data outside of Ghana.

The Data Protection Act carves out personal data relating to children as sensitive data.[131] The Children's Act defines a child as a person under the age of 18.[132] The Data Protection Act prohibits, unless other provisions apply, the processing of data relating to a child.

The Data Protection Act allows the processing of data relating to a child for medical purposes. It also allows for "necessary" processing, such as by schools and in other matters related to education.

Hong Kong

The Personal Data Privacy Ordinance (PDPO)[133] is Hong Kong's principle legal instrument governing data privacy. The PDPO regulates the collection, storage, processing and use of personal data based on six data protection principles.[134] The Personal Data (Privacy) (Amendment) Ordinance,[135] which significantly amends the PDPO, governs personal data in direct marketing. Further amendments to the PDPO, which primarily address the issue of disclosing data without consent, were introduced in 2021 pursuant to the Personal Data (Amendment) Ordinance 2021.

The PDPO does not specifically address children's data privacy, however, it establishes requirements for parental consent in certain circumstances. Where the data subject is a minor (i.e., under the age of 18), any prescribed consent required for using personal data for a new purpose may be provided on the child's behalf by an individual who has parental responsibility for them.[136] The person with parental responsibility may also request access and the opportunity to correct data on behalf of a minor.

The Office of the Privacy Commissioner for Personal Data has issued guidance focused on children's data. This guidance addresses appropriate collection and processing, privacy issues raised by online discussion forums, parental involvement, deleting account or personal data, default privacy settings, disclosure of personal data, the need for consent when a change in use of personal data is anticipated, issues raised by social networks, direct marketing, security, transparency and privacy controls.[137]

In response to concerns about the collection and processing of data generated on online video conferencing platforms, the PDPO issued guidance in 2020 that addresses children's privacy in the context of education.[138]

India

While the Constitution of India (the Constitution) recognizes a fundamental right to privacy, India's privacy framework is not well developed, and no law specifically addresses the protection of individuals' personal data. However, India does have in place laws and policies that provide a baseline for children's protection online.[139]

There is no uniform code or law in India that deals with obtaining consent for the processing of children's data.

Several policies in India apply to national, state and local governments and address the protection of children in education. The National Policy for Children,[140] for example, requires all state policies related to education, information, and communications technology and cybersecurity incorporate principles that reflect the need to protect children while promoting their empowerment and learning opportunities. The National Policy of Information and Communications Technology in Schools[141] governs student tracking for academic purposes and promotes children's safety through the monitoring of IT systems.

Israel

The Protection of Privacy Law (PPL) governs data protection in Israel.[142] The PPL addresses the collection and processing of personal data and sensitive data. Regulations have been promulgated pursuant to the PPL,[143] and the Privacy Protection Authority (PPA) acts as enforcer.

Guidance issued by the PPA states that a parent or guardian must consent to the collection of personal data regarding a child—a data subject under the age of 14. When sensitive data regarding a minor—a data subject under age 18—the consent of a parent or guardian is required.

Japan

The Act on the Protection of Personal Information (Act No. 57 of 2003) (APPI)[144] governs the protection of personal data in Japan. The APPI aligns with traditional articulations of fair information practices principles.[145]

The APPI does not include provisions that specifically regulate the processing of children's data. However, the General Guidelines on the APPI[146] issued by Japan's Personal Information Protection Commission[147]

indicate that, if a minor, adult ward or person under curatorship has no capacity to understand the meaning of their consent as provided for in the APPI, consent should be obtained from their statutory guardians. The PPC further notes that, while the age at which children can understand the significance of their consent should be considered on a case-by-case basis, as a general matter consent should be obtained from a statutory guardian (e.g., a parent) when a child is under the age of 15.

There is no law in Japan governing children's data in education settings.

Malaysia

Data protection in Malaysia is governed primarily by the Personal Data Protection Act 2010 (PDPA)[148] and related legislation. The PDPA requires that data users comply with certain obligations and confers on the data subject certain rights with respect to personal data.

In general, the PDPA provides that a "data user" may not process a data subject's personal data without their consent. Under the PDPA, children (minors under the age of 18) cannot consent to the processing of their personal data. Regulations issued in 2013[149] require that consent be obtained from the parent, guardian or person who has parental responsibility for the minor. The Child Act 2001 defines a child as a person under the age of 18.[150] Consent must be provided in a form that can be properly recorded and maintained by the data user.

Malaysia has not enacted laws or regulations that apply to privacy in the context of children's education.

The Personal Data Protection Code of Practice for Licensees under the Communications and Multimedia Act 1998 (CMA Code)[151] governs requests for access to children's data. A parent, guardian or person with parental responsibility may make such a request access on behalf of the child.

New Zealand

The Privacy Act (2020) (the 2020 Act) governs data protection in New Zealand.[152]

The 2020 Act states that a company may only collect personal data which under the circumstances is fair and does not unreasonably intrude upon the individual's personal affairs. This rule applies particularly when personal data is being collected from children or young people.[153]

The 2020 Act does not define the age below which a person is considered a child.

The Privacy Commissioner has suggested a 'practical approach' when considering how to treat personal data relating to children, particularly where the children are not old enough to act on their own. In such cases, it may be appropriate to treat the child's parent or guardian as their representative.[154]

The Health Code provides that parents and guardians of individuals under the age of 16 may request their child's health data. This provision does not apply to personal data generally.

Russia

Data protection in Russia is provided through a myriad of Acts, Regulations, Decrees and Conventions. Among these are the Russian Constitution,[155] the Convention for the Protection of Individuals with regard

to Automatic Processing of Personal Data 108.81[156] and an amending protocol. Additional laws, orders and decrees address specific matters such as security, biometrics, artificial intelligence, processing and storage of data and drafting a privacy policy.

Russia's data protection laws do not specifically address the processing of children's data.

Russian law establishes 18 as the age of majority and provides that the rights of minors are exercised by their parents or legal representatives. Thus, when it is required, consent to the processing of children's data must be obtained from a parent or guardian. Some exceptions may apply, however, when a child reaches the age of 14.

South Africa

The Protection of Personal Information Act, 2013 (POPIA)[157] governs, with certain exceptions, the processing of personal data in South Africa.

The POPIA affords children's personal data special protections. It prohibits the processing of personal data concerning a child[158] and states that the general prohibition will not apply when processing is:

- carried out with a parent or guardian's consent;
- necessary to establish, exercise or defend a right or obligation in law;
- necessary to comply with an international public law; or
- with some conditions, for historical, statistical or research purposes.[159]

A business must obtain prior authorization from the South African data protection authority when transferring personal data of children from South Africa to a third party in a foreign country, where that country does not provide an adequate level of protection for the processing of personal data, whether in law, binding corporate rules or other mechanism to establish principles substantially similar to the conditions for lawful processing found in POPIA.[160]

South Korea

The Personal Information Protection Act 2011[161] (the PIPA) and its implementing regulations govern the collection, processing and disclosure of personal data by government, private entities and individuals. In almost all cases, the data subject's consent is required to process their personal data.

The PIPA establishes that a legal representative must consent to the processing of personal data of children under the age of 14.[162] It also provides that data processors may collect from the child data needed to obtain such consent, but only to the extent necessary to do so.[163]

Information and communications service providers (ICSP) are required to notify children in a clear, easily understandable way about the processing of their personal data. They also must obtain the legal representative's consent if the ICSP wishes to collect or use the personal data of a child under 14, and to confirm that the consent was provided as prescribed by statute.[164]

Singapore

The Personal Data Protection Act[165] (PDPA) governs the collection, use and disclosure of personal data in Singapore. The Personal Data Protection Commission (PDPC) administers the law.

The PDPA requires that that organizations can collect, use or disclose personal data about an individual only with his or her consent.[166] The PDPA does not address children's data specifically.

In its Selected Topic Guidelines,[167] however, the PDPC addresses the issue of children's consent. It recommends that in determining whether a minor can effectively provide consent on his or her own behalf, organizations consider whether a minor sufficiently understands the nature of consent and its consequences.[168] However, as a general matter, the PDPC considers any child over the age of 13 as capable of understanding and consenting.[169] The PDPC also recommends that when obtaining consent from children under age 13 or where it appears that the child does not adequately understand the nature and consequences of their consent, the child's parent, guardian or person legally able to do so should consent on their behalf.[170]

There is no law in Singapore that specifically addresses children's privacy in education.

Philippines

The Data Privacy Act of 2012[171] (the Act) is the comprehensive data privacy law in the Philippines. The National Privacy Commission (NPC),[172] established in early 2016, issued Implementing Rules and Regulations of Republic Act 10173 (IRR).[173] The IRR sets forth detailed requirements related to processing personal data and sanctions for violations of the Act.

The Act defines 15 as the age of consent to the processing of personal data. This applies where information society services are provided and offered directly to a child.

The NPC has stated in several official opinions that children merit specific protections. [174] A parent or legal guardian's consent, therefore, must be obtained before the personal data of minors may be lawfully processed. If consent is not obtained, a legal basis must be established prior to processing.

Taiwan

Personal Data Protection Act 2015 (PDPA)[175] and the Enforcement Rules of the Personal Data Protection Act[176] are the primary legal instruments governing data protection in Taiwan.

The age of majority in Taiwan is 18. While the PDPA does not address collection of data from minors specifically, the Taiwan Civil Code[177] Minors establishes two categories of minors—children over and under the age of seven. It provides that that children under the age of seven have no capacity to make "juridical acts," while minors over seven do.[178] Thus, any consent to collect or process personal data provided by a minor over the age of seven is invalid without the approval of a "holder of parental responsibility". For children under the age of 7, only the holder of parental responsibility has authority to provide consent.

Thailand

The Personal Data Protection Act 2019 (PDPA) governs data protection in Thailand. The Thai Civil and Commercial Code[179] entitles individuals to claim damages under tort law if data is used in violation of an individual's right to privacy under the Constitution. Any use of personal data in a way that violates an individual's rights as recognized by the Constitution may entitle them to claim damages under tort law.

Thailand considers persons under the age of 20 to be minors. If the data subject is a minor, the data controller is required to make special provisions for consent, depending on the minor's age. The data controller must:

- obtain parental consent for minors who have not reached the age of 10;
- obtain only the minor's consent when that person is between the ages of 10 and 20, in instances where the minor is competent to consent; and
- obtain both parental consent and the consent of minors between the ages of 10 and 20 in instances where minors are not competent to give consent.

Requests for consent: (i) must be in writing or via electronic means, (ii) must be clearly separated from other messages, (iii) must be delivered in a format which is easily accessible and understandable; and (iv) should not mislead the data subject. Consent must be freely given and not a condition of the contract.

Vietnam

Data protection is addressed in several rules and regulations, including the Civil Code[180], the Law on Cybersecurity[181] and in sectoral laws, such as the Law on Electronic Transactions[182] and the Law on Telecommunications[183], govern data protection in Vietnam.

The Law on Children[184] prohibits the disclosure of personal data of a child under 8 years old without the consent of the child's parents or guardian.[185] Additionally, the Cybersecurity Law states that "[c]hildren have the right to be protected; to access information; to participate in social, entertainment and recreational activities; to keep their personal secrets confidential" and other rights when they participate in cyberspace".[186]

Information systems, telecommunication service providers and internet service providers are charged with ensuring that information on their systems is not harmful to children and does not violate children's rights, blocking and deleting information that is harmful to children or that violates children's rights, and informing and cooperating with authorities whenever such information is detected. Agencies, organizations, parents, teachers, caregivers and other relevant individuals are responsible for protecting children from harm and for ensuring their rights while participating on cyberspace as articulated in laws related to children.[187]

United Kingdom

The UK General Data Protection Regulation[188] (UK GDPR) and the Data Protection Act 2018 (the Act) govern data protection in the UK.

The UK GDPR provides specific protections for children. It establishes that children 13 and under cannot provide valid consent to the processing of their data when they are offered an information society service and consent is required. In such cases, parental consent is necessary. Where data have been collected by an information society service based on the child's consent, the individual can exercise their right to erasure.[189] Organizations are also required to carry out data protection impact assessments in cases of high-risk processing.[190] The ICO's Guidance on DPIAs notes that data processing involving children will likely be classified as high risk and require the completion of a DPIA.[191]

The ICO details protections for children in more detail in guidance, "Children and the UK GDPR".[192] It explains that a person with parental responsibility for a child is someone who has the legal rights and responsibilities related to a child that are normally afforded to parents, as provided for in the law where the child resides. It notes that such a person "will not always be a child's 'natural parents' and parental responsibility can be held by more than one natural or legal person".[193]

The ICO recently has also published the UK's *Age Appropriate Design: A Code of Practice for Online Services*, a statutory code of practice which addresses issues relating to the processing of children's data and design of an ISS. The Code is discussed elsewhere in this paper.

United States

Privacy in the United States is governed by a mosaic of national, state and local privacy laws and regulations. While there is no comprehensive national privacy law, the US has in place federal level sector-specific laws privacy and data security laws.[194] Additional laws are in place at the state level.

The privacy of children's data is governed by Children's Online Privacy Protection Act (COPPA)[195] a federal law that applies to personal data collected online from children.[196]

COPPA requires that, prior to collecting the personal data of a child under the age of 13,[197] companies notify parents and obtain their consent.[198] COPPA also requires companies to minimize the data collected and enable parents to review and delete it.[199] Companies are required to secure the data and to dispose of it when it is no longer needed.

COPPA is enforced by the US Federal Trade Commission (FTC) and state attorneys general. It provides for development by industry of self-regulatory guidelines that would establish safe harbor programs and articulates criteria for their approval by the FTC. Organizations that meet the requirements of approved self-regulatory programs are deemed in compliance with COPPA.[200]

In addition to COPPA, two states have enacted laws that specifically address children's online privacy. California enacted Privacy Rights for California Minors in the Digital World.[201] Among other provisions, the law prohibits an operator of a Web site or online service directed to minors from marketing or advertising to minors specified products or services that minors are legally prohibited from buying. The law also prohibits marketing or advertising certain products based on personal data specific to a minor or knowingly using, disclosing, compiling or allowing a third party to do so. Most recently, it passed the California Age Appropriate Design Code Act, which places new legal obligations on companies with respect to online products and services that are "likely to be accessed by children" under the age of 18.[202]

The state of Delaware prohibits operators of websites, online or cloud computing services, online applications, or mobile applications directed at children from marketing or advertising on its Internet service specified products or services inappropriate for children's viewing, such as alcohol, tobacco, firearms or pornography.[203] The law also prohibits an operator of an Internet service who has actual knowledge that a child is using the Internet service from using the child's personally identifiable data to market or advertise the products or services to the child, and also prohibits disclosing a child's personally identifiable data if it is known that the child's personally identifiable data will be used for the purpose of marketing or advertising those products or services to the child.

Appendix Two: National Law Affecting Children's Data Privacy

Country	Privacy Law	Applicable Legislation	Supervisory Authority and Regulatory Guidance	Children's Specific Legislation
Argentina	Personal Data Protection Law (PDPL) Decree 1558 of 2001	National Civil and Commercial Code National Criminal Code	Argentine data protection authority (AAIP) Resolution 4/2019— *"Guiding criteria and indicators of best practices in the application of the Act"* (the AAIP Criteria)	
Australia	Privacy Act 1988 (No. 119, 1988)		Office of the Australian Information Commissioner "Australian Privacy Principles"	Mix of general privacy legislation, online safety regulation and legislation that does not address privacy but rather imposes obligations related to confidentiality and record handling
Austria	GDPR	Federal Act concerning the Protection of Personal Data	Austrian Data Protection Authority	
Belgium	GDPR	Act of 30 July 2018 on the Protection of Individuals with Regard to the Processing of Personal Data	Data Protection Authority	
Bolivia	Does not have a general data protection law in place	Telecommunications Law No. 164 of 8 August 2011 Supreme Decree No. 1391 General Consumer Rights Law 2013 Supreme Decree No. 28168/2005	Agency of the electronic government and information technologies and communication (AGETIC)	The Code of the Boy, Girl and Adolescent (Law No. 548 of November 2018)
Brazil	General Personal Data Protection Law (LGPD)		Brazilian data protection authority (ANPD)	Child and Adolescent Statute
Bulgaria	GDPR	Bulgarian Personal Data Protection Act	Commission for Personal Data Protection	
Canada	Personal Information Protection and Electronic Documents Act 2000 (PIPEDA)	British Columbia Personal Information Protection Act Alberta's Personal Information Protection Act Quebec's Act respecting the Protection of Personal Information in the Privacy Sector	Office of the Privacy Commissioner of Canada (and of Alberta, British Columbia and Quebec) "Collecting from kids? Ten tips for services aimed at children and youth" "Guidelines for obtaining meaningful consent"	

Country	Privacy Law	Applicable Legislation	Supervisory Authority and Regulatory Guidance	Children's Specific Legislation
China	Personal Information Protection Law (PIPL)	Cybersecurity Law Data Security Law Civil Code		Cyber Protection of Children's Personal Information
Colombia	Statutory Law 1581 of 2012 Data Protection Law	Statutory Law 1266 of 2008	Under Law 1581, the Superintendent of Industry and Commerce is the highest authority regarding personal data protection and data privacy	Colombia's Decree 1377 of 2013
Croatia	GDPR	Act on Implementation of the General Data Protection Regulation	Personal Data Protection Agency	
Cyprus	GDPR	Law 125(I) of 2018 Providing for the Protection of Natural Persons with Regard to the Processing of Personal Data and for the Free Movement of Such Data	Commissioner for the Protection of Personal Data	
Czech Republic	GDPR	Act No. 110/2019 Coll. on the processing of personal data	Office for Personal Data Protection	
Denmark	GDPR	Danish Data Protection Act	Danish Data Protection Agency	
Egypt	Law on Data Protection		Personal Data Protection Centre	Child Law No. 12 of 1996
Estonia	GDPR	Personal Data Protection Act	Data Protection Inspectorate	
European Union	GDPR	Directive on Privacy and Electronic Communications (ePrivacy Directive) Audio-visual Media Services Directive (AVMSD) Digital Services Act (DSA) *forthcoming*		
Finland	GDPR	Data Protection Act 1050/2018	Office of the Data Protection Ombudsman	
France	GDPR	Act No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (as amended)	National Commission on Informatics and Liberty (CNIL) The Digital Rights of Children	
Germany	GDPR	Federal Data Protection Act	Federal Commissioner for Data Protection and Freedom of Information (acts as representative for Landers' authorities)	Youth Protection Act
Ghana	Data Protection Act		Data Protection Commission (DPC)	
Greece	GDPR	Law No. 4626/2019	Hellenic Data Protection Authority	

Country	Privacy Law	Applicable Legislation	Supervisory Authority and Regulatory Guidance	Children's Specific Legislation
Hong Kong	Personal Data Privacy Ordinance (PDPO)	Personal Data Ordinance 2021 and further amendments	Office of the Privacy Commissioner for Personal Data "Collection and Use of Personal Data through the Internet—Points to Note for Data Users Targeting at Children", December 2015 "PCPD Provides Guidelines on Children's Privacy during the Pandemic," April 2, 2022	
Hungary	GDPR	Information Self-Determination and Freedom of Information Act	Hungarian Data Protection Authority	
India	Forthcoming Personal Data Protection Bill 2021			National Policy for Children
Ireland	GDPR	Irish Data Protection Law	Data Protection Commissioner (DPC) of Ireland Fundamentals for a Child-Oriented Approach to Data Processing	
Israel	Protection of Privacy Law and regulation pursuant to it		Privacy Protection Authority (PPA)	
Italy	GDPR	Personal Data Protection Code	Italian Data Protection Authority	
Japan	The Act on the Protection of Personal Information (Act No. 57 of 2003) (APPI)		Japan's Personal Information Protection Commission ***General Guidelines on the APPI***	
Latvia	GDPR	Personal Data Protection Law	Data State Inspectorate	
Lithuania	GDPR	Law on Legal Protection of Personal Data of the Republic of Lithuania	State Data Protection Inspectorate	
Luxembourg	GDPR	Act of 1 August 2018 on the implementation of GDPR	National Data Protection Commission	
Malaysia	Personal Data Protection Act 2010 (PDPA)	Personal Data Protection Code of Practice for Licensees under the Communications and Multimedia Act 1998 (CMA Code)	Personal Data Protection Commissioner and Personal Data Protection Advisory Committee	Child Act 2001
Malta	GDPR	Maltese Data Protection Act 2018 (Chapter 586 of the Laws of Malta)	Information and Data Protection Commissioner	
Netherlands	GDPR	Dutch GDPR Implementation Act	Dutch Data Protection Authority "Code for Children Rights"	
New Zealand	The Privacy Act (The 2020 Act)	Health Code	Privacy Commissioner's Office	
Philippines	Data Privacy Act of 2012	Implementing Rules and Regulations of Republic Act 10173 (IRR)	National Privacy Commission (NPC)	
Poland	GDPR	New Data Protection Act	Personal Data Protection Office	

Country	Privacy Law	Applicable Legislation	Supervisory Authority and Regulatory Guidance	Children's Specific Legislation
Portugal	GDPR	Law No. 58 of 2019 Portuguese Data Protection Law	National Data Protection Commission	
Romania	GDPR	Data Protection Law No. 190 of 18 July 2018 on the implementation of the GDPR	National Supervisory Authority for Personal Data Processing	
Russia	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 108.81 and amending protocol	Russian Constitution	Federal Service for Supervision of Communications, Information Technologies and Mass Media	
Singapore	Personal Data Protection Act (PDPA)		Personal Data Protection Commission (PDPC) "Advisory Guidelines on the Personal Data Protection Act for Selected Topics"	
Slovakia	GDPR	Act No. 18/2018 Coll. on the protection of personal data and on amendments to certain acts	Office for Personal Data Protection	
Slovenia	GDPR	Slovenian Data Protection Act ZVOP-1 ZVOP-2 at the stage proposal	Information Commissioner	
South Africa	Protection of Personal Information Act, 2013 (POPIA)	The Constitution	Information Regulator	
South Korea	Personal Information Protection Act 2011 and its implementing regulations		Personal Information Protection Commission (PIPC)	
Spain	GDPR	Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (LPDP)	Spanish Data Protection Agency	
Sweden	GDPR	Law on Additional Provisions to the EU Data Protection Regulation	Swedish Authority for Privacy Protection "The rights of children and young people on digital platforms"	
Taiwan	Personal Data Protection Act 2015 (PDPA) and the Enforcement Rules of the Personal Data Protection Act	Taiwan Civil Code	National Development Council	Taiwan Civil Code
Thailand	Personal Data Protection Act 2019 (PDPA)	Constitution Civil and Commercial Code	Personal Data Protection Committee (PDPC)	

Country	Privacy Law	Applicable Legislation	Supervisory Authority and Regulatory Guidance	Children's Specific Legislation
UK	UK GDPR Data Protection Act 2018		Information Commissioner Officer	Age-Appropriate Design: A Code of Practice for Online Services
United States	Children's Online Privacy Protection Act (COPPA)	Privacy Rights for California Minors in the Digital World Delaware Code	COPPA is enforced by the US Federal Trade Commission (FTC) and state attorneys general	
Vietnam	No single law governs data protection	Civil Code, Law on Cybersecurity, Law on Electronic Transactions, Law on Telecommunications		Law on Children

Appendix Three: Select Codes of Conduct and Regulator Guidance[204]

1. UK Age Appropriate Design: A Code of Practices for Online Services—An Enforceable Code from the UK Information Commissioner's Office

In 2021, the UK ICO published *Age-Appropriate Design: A Code of Practices for Online Services* (The Code).[205] The Code is a statutory code of practice[206] designed so that conforming to it will ensure that an organization providing online services likely to be accessed by children in the UK will take into account the best interests of the child, providing them with protections as well as the opportunity to explore and develop online.

The code sets out 15 standards of age-appropriate design that reflect a risk-based approach to protection. The first of these standards states that, "The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child".[207] It instructs companies to conduct a data protection impact assessment (DPIA) "to mitigate the risks that arise from data processing to the rights and freedoms of children" who are likely to access their services. In doing so, companies are to consider the differing ages, capacities and developmental needs of children and ensure that the DPIA builds in compliance with the Code. It also requires that a company's privacy setting be set to "high" by default, unless it can demonstrate a compelling reason for a different default setting, taking into account the standard of the best interests of the child.[208]

The ICO also published its "Opinion on Age Assurance".[209] The Opinion is directed toward providers of information society services (ISS) in scope of the code, and providers of age assurance products, services and applications that those ISS may use to conform with the Code. It sets out how the Commissioner currently expects ISS to meet the code's age-appropriate application standard. The Opinion outlines a risk-based approach for organizations to apply age assurance measures that are appropriate for their use of children's data and organizational context.

2. Fundamentals for a Child-Oriented Approach to Data Processing—Guidance from the Irish Data Protection Authority

The Data Protection Commission (DPC) of Ireland published *Fundamentals for a Child-Oriented Approach to Data Processing* (Fundamentals),[210] designed "to drive improvements in standards of data processing". They establish the best interests of the child as the primary consideration in all decisions relating to the processing of their data.[211]

Unlike the UK's Code, the *Fundamentals* are not enforceable. However, the DPC states that they "set the marker for organizations that process children's data *by establishing baseline expectations of the DPC* as the regulator for the processing of personal data of children in Ireland, and also as the lead supervisory authority under the GDPR for multinational organizations processing the personal data of EU children whose main or single establishment in the EEA is in Ireland". (emphasis added) The Fundamentals introduce 14 child-specific data protection interpretative principles and, like the UK Code, recommend that organizations carry out DPIAs. They encourage measures to enhance protections for children against data processing risks, both on and offline. The Fundamentals are also intended to assist organizations that process children's data, by clarifying the principles arising from the high-level obligations under the GDPR to which the DPC expects such organizations to adhere. In addition to DPIAs, the principles call for requirements for clear consent when it is the appropriate legal basis for processing, establishment of privacy by design and default processes, and transparency mechanisms that serve the needs of children. The Fundamentals direct organizations to "know your audience" and to "take steps to identify their users and ensure that services directed at/intended for or likely to be accessed by children have child-specific data protection measures in place".[212]

The Fundamentals also address in detail issues related to the age of consent (in Ireland, age 16), obtaining and verifying parental consent, and age verification. They include criteria for a risk-based approach to age verification in the context of data collection that includes considerations such as the type and sensitivity of the data, the service being provided, the accessibility of the data to other persons, and whether and for what reasons the data may be shared with other organizations.[213]

3. The Digital Rights of Children—Guidance from the CNIL

After conducting a comprehensive review of data protection for children, France's data protection authority, the CNIL, published The Digital Rights of Children[214]—eight guidelines intended to provide practical advice and to clarify aspects of legal requirements related to children's data. The CNIL also noted the importance of the guidelines to parents and other participants online and called upon lawmakers to be mindful of them as they consider legislation.

The recommendations are directed toward children, parents and educators, and online service providers. Like the Code and the Fundamentals, they highlight the best interests of the child, and the need to consider children's evolving need to develop personal autonomy and exercise their rights while protecting them online. At the same time, they recognize the role of parents and educators in supporting children in the digital environment. But they are also designed to make online service providers aware of their increased responsibility toward children when processing their personal data.

Service providers are advised to:

1. take into account the capacity of children to act online;
2. encourage children to exercise their rights;
3. support parents with digital education;
4. seek parental consent for children under 15;
5. promote parental controls that respect the child's privacy and best interests;
6. strengthen the information and rights of children by design;
7. check the age of the child and parental consent while respecting the child's privacy;
8. provide specific safeguards to protect the interests of the child.[215]

The CNIL has indicated that it envisions these recommendations as the starting point of the CNIL's work in this area. The CNIL notes that some of them "open the way to cooperation with those involved, in order to help them become technically operational and to suggest practical advice and appropriate teaching resources". It anticipates new recommendations as it develops this work further in specific areas such as the educational, medical, banking or judicial fields that raise challenging legal questions[216].

Appendix Four: Age of Consent and Verification of Consent Requirements

Country	Age of Consent	Consent Requirements	Companies' Obligations to Verify Consent
Argentina	National Civil and Commercial Code: Under 18 years old lack the capacity to exercise their rights AAIP Criteria: Under 13 years old cannot perform "voluntary rightful acts" Over 13 can if they are mature enough	If a minor does not have sufficient capacity to provide informed consent, consent must be obtained from a parent or guardian	The data controller must make reasonable efforts to verify that the consent was given by the holder of parental responsibility
Australia	Privacy Act: does not specify the age of consent. OAIC Guidance: Under 18 may give consent if has sufficient understanding and maturity to understand the particular processing	For under 18 and those who have not sufficient maturity or understanding, parent or guardian consent may be appropriate	Entities subject to the Privacy Act must assess on a case-by-case basis whether the individual has the capacity to consent. Where it is not practicable, the entity may presume that a data subject over the age of 15 has capacity to consent, unless there is something to suggest otherwise
Austria	14 years old	For under 14, consent is given by the holder of parental responsibility for the child	
Belgium	13 years old	For under 13, consent is given by the holder of parental responsibility for the child	
Bolivia	Persons under the age of 18 are unable to give consent		Organizations must protect children's personal data, unless there is an express authorization from the competent authority
Brazil	18 years old Child is any person up to 12 years of age, and an adolescent is any person between 13 and 18 years of age	Parental consent is required for all processing activities involving children's data	All reasonable efforts should be made to verify that consent has been provided by the parent responsible for the child, bearing in mind the technologies available to support consent Children's data may be collected without parental consent, however, in certain circumstances, i.e., when collection is necessary to contact the parent or legal guardian or for the child's protection

Country	Age of Consent	Consent Requirements	Companies' Obligations to Verify Consent
Bulgaria	14 years old Children aged 14 to 18 years have limited legal capacity and the validity of their legal acts and transactions are subject to the prior consent of their parents or legal guardians, except for minor transactions relating to children's on-going and customary needs	For under 14, consent is given by the holder of parental responsibility for the child For children aged between 14 and 18, consent-based processing of personal data will often require the prior consent of the child's parent or legal guardian	
Canada	The OPC takes the position that, in all but exceptional circumstances, anyone under the age of 13 is unable to provide meaningful consent	For under 13, organizations must obtain consent from a parent or guardian	Organizations should ensure that the consent process for youth able to provide consent themselves reasonably considers their level of maturity Organizations should stand ready to demonstrate on demand that their chosen process leads to meaningful and valid consent
China	PIPL: Children are defined as minors under the age of 14 Cyber Protection of Children's Personal Information: Define children as minors under 14 years old	For under 14, organizations must obtain the consent of the parent or other guardian	The Provisions set up a higher standard of consent than the Cybersecurity Law of China. Network operators who wish to obtain informed consent from a guardian, must provide a mechanism whereby consent can be declined
Colombia	DPL: 18 years old Decree 1377 of 2013 allows minor's data processing when necessary for the protection of fundamental rights	For under 18, organizations must obtain the consent of the parent or other guardian	
Croatia	16 years old	For under 16, organizations must obtain the consent of the parent or other guardian	
Cyprus	14 years old	For under 14, organizations must obtain the consent of the parent or other guardian	
Czech Republic	15 years old	For under 16, organizations must obtain the consent of the parent or other guardian	
Denmark	13 years old	For under 13, organizations must obtain the consent of the parent or other guardian	
Egypt	18 years old	For under 18, organizations must obtain the consent of the parent or other guardian	
Estonia	13 years old	For under 13, organizations must obtain the consent of the parent or other guardian	
European Union	16 years old	For under 16, organizations must obtain the consent of the parent or other guardian	Organizations must make reasonable efforts to verify that the holder of parental responsibility has consented

Country	Age of Consent	Consent Requirements	Companies' Obligations to Verify Consent
Finland	13 years old	For under 13, organizations must obtain the consent of the parent or other guardian	
France	15 years old	For under 15, organizations must obtain the consent of the parent or other guardian	CNIL's Guidance to checking parental authorization include declaration, certification and AI methods
Germany	16 years old	For under 16, organizations must obtain the consent of the parent or other guardian	
Ghana	18 years old The Data Protection Act allows processing of data relating to a child when processing is related to medical purposes and when processing is necessary and when it relates to medical purposes	The Data Protection Act prohibits the processing of data relating to a child who is under parental control unless otherwise provided by the Data Protection Act.	
Greece	15 years old	For under 15, organizations must obtain the consent of the parent or other guardian	
Hong Kong	18 years old	For under 18, organizations must obtain the consent of the individual who has parental responsibility	
Hungary	16 years old	For under 16, organizations must obtain the consent of the parent or other guardian	
India	Forthcoming Personal Data Protection Bill 2021	Organizations will need to obtain the consent of the individual who has parental responsibility	Organizations will have to put in place age verification
Ireland	16 years old	For under 16, organizations must obtain the consent of the parent or other guardian	The "reasonable efforts" that organizations must take to verify the giving of parental consent depends on the nature of the processing and the risks associated with it. The Irish DPC considers that a higher burden applies to business whose models are predicated on deployment of digital and online technologies
Israel	Guidance issued by the PPA Minors: children under 18 years old Child: data subject under the age of 14	Informed consent from parent or guardian is required for collection of personal data regarding a child and collection of sensitive data regarding a minor	
Italy	14 years old [contract law doesn't allow minors to enter into contracts earlier]	For under 14, consent must be given or authorized by the holder of parental responsibility	
Japan	15 years old, BUT the age at which children can understand the significance of their consent should be considered on a case-by-case basis	For under 15, and if the minor has no capacity to understand the meaning of their consent, it should be obtained from their statutory guardians.	
Latvia	13 years old	For under 13, organizations must obtain the consent of the parent or other guardian	

Country	Age of Consent	Consent Requirements	Companies' Obligations to Verify Consent
Lithuania	14 years old	For under 14, consent is given by the holder of parental responsibility for the child	
Luxembourg	16 years old	For under 16, organizations must obtain the consent of the parent or other guardian	
Malaysia	Children, minors under 18 years old, cannot consent to the processing of their personal data	For under 18, organizations must obtain the consent of the parent or other guardian	Consent must be provided in a form that can be properly recorded and maintained by the data user
Malta	13 years old	For under 13, organizations must obtain the consent of the parent or other guardian	
Netherlands	16 years old	For under 16, organizations must obtain the consent of the parent or other guardian	
New Zealand	The 2020 Act does not define the age below which a person is considered a child. The Privacy Commissioner has suggested a 'practical approach' when considering how to treat personal data relating to children, particularly where the children are not old enough to act on their own	In such cases, it may be appropriate to treat the child's parent or guardian as their representative. The Health Code provides that parents and guardians of individuals under the age of 16 may request their child's health data. This provision does not apply to personal data generally	
Philippines	15 years old	For under 15, organizations must obtain the consent of the parent or other guardian Absent such consent, prior to the processing of a minor's personal data a legal basis must be established under existing laws, rules, or regulations	
Poland	16 years old	For under 16, organizations must obtain the consent of the parent or other guardian	
Portugal	13 years old	For under 13, consent is given by the holder of parental responsibility for the child	Company must obtain permission from a legal guardian through a secure means of authentication
Romania	16 years old	For under 16, organizations must obtain the consent of the parent or other guardian	
Russia	18 years old. In certain cases children may, beginning at age of 14, act somewhat independently, e.g., when engaging in small transactions	When consent is required, it must be obtained from parents or other legal representatives	
Singapore	The PDPC considers any child over the age of 13 as capable of understanding and consenting It also recommends that organizations consider whether a minor sufficiently understands the nature of consent and its consequences	For under 13 or where it appears that the child does not adequately understand the nature and consequences of their consent, the child's parent, guardian, or person legally able to do so should consent on their behalf	Organizations are advised to verify the accuracy of children's data, particularly where its processing may have serious consequences for the child

Country	Age of Consent	Consent Requirements	Companies' Obligations to Verify Consent
Slovakia	16 years old	For under 16, organizations must obtain the consent of the parent or other guardian	
Slovenia	16 years old [likely to be reduced to 15 (or 14) years of age under the current ZVOP-2 proposal]	For under 16, organizations must obtain the consent of the parent or other guardian	
South Korea	14 years old	For under 14, a legal representative must consent to the processing	Companies must confirm that the legal representative granted consent in the statutorily prescribed manner
South Africa	18 years old (who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself)	Personal information may only be processed if the data subject or a competent person where the data subject is a child consents to the processing;	The responsible party bears the burden of proof for the data subject's or competent person's consent
Spain	14 years old	For under 14, consent is given by the holder of parental responsibility for the child	
Sweden	13 years old The Data Protection Authority suggests that the age limit needs to be balanced between the right to be included and the risk of the child being harmed	For under 13, consent is given by the holder of parental responsibility for the child	
Taiwan	Age of majority in Taiwan is 18 Civil Code: Children under the age of seven have no capacity to make "juridical acts," minors over seven do	Any consent to collect or process personal data provided by a minor over the age of seven is invalid without the approval of a "holder of parental responsibility" For children under the age of 7, only the holder of parental responsibility has authority to provide consent	
Thailand	Thailand considers persons under the age of 20 to be minors	The data controller must: obtain parental consent for minors between the ages of 0 and 10 obtain only minor's consent for minors who are older than 10 but younger than 20 years of age for an act for which minors are competent to give consent obtain both parental consent and the consent of the minors who are older than 10 but younger than 20 years for an act for which minors are not competent to give consent	The Data Controller must also ensure that the consent is freely given and not conditional on entering into a contract
UK	13 years old	For under 13, consent is given by the holder of parental responsibility for the child	[Age Assurance measures and tools]
United States	COPPA sets the age at 13	In COPPA, for under 13, companies are required to notify parents and obtain their consent	
Vietnam		The Law on Children prohibits the disclosure of personal data of a child under 8 years old without the consent of the child's parents or guardian	

References

1 CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 90 member organisations that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth. Moreover *The descriptions of relevant legal requirements and standards contained in this paper, including in the appendixes, are provided for reference and illustrative purposes and are not intended to be comprehensive or intended to serve as legal advice. The quickly evolving nature of relevant laws may impact the accuracy and completeness of these summaries. For specific questions on laws concerning children's data and privacy, legal counsel should be consulted.*

2 "*The State of the World's Children 2017: Children in a Digital World*", UNICEF, p. 35, available at https://www.unicef.org/media/48601/file.

3 This variation in requirements is illustrated in Appendices One and Three, and in the tables found in Appendices Two and Four.

4 The need for children to learn to think critically and to exercise autonomy in their online decisions and activity may argue for establishing a lower age of consent, at least for some activities online, that allows for that development.

5 Age verification raises questions of accuracy of outcomes, how they may be used in a way that the level of accuracy is proportional to the risks to the child posed by the data collection or content, and how they may be used as part of a risk-based approach to protecting children.

6 Such tensions exist in the physical world as well. Children inevitably test boundaries; parents struggle with lack of familiarity with their children's interests, e.g., new music, controversial subject matter in films, computer games, etc. In some cases, these involve risk and parents face challenges in supervising their children and helping them navigate that risk.

7 Ibid. In Artificial intelligence and privacy, and children's privacy, the UN General Assembly notes that "[t]raditionally, the privacy rights of children have been regarded as an issue for adults to determine. Children's privacy needs, however, differ from and can conflict with those of adults". It also notes that adults understanding of what children need with respect to privacy can "impede the healthy development of autonomy and independence and restrict children's privacy in the name of protection."

8 A discussion of guidance that relies on an assessment of the best interests of the child, e.g., the UK's Age Appropriate Design Code and the Irish Data Protection Commission's Fundamentals for a Child-Oriented Approach to Data Privacy is provided later in this paper.

9 European Strategy for a Better Internet for Kids, May 2022, available at https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids.

10 Audio-Visual Services Directive, Directive (EU) 2018/1808, available at https://eur-lex.europa.eu/eli/dir/2018/1808/oj. Article 6(a) of the AVSD requires that EU Member States take appropriate measures to ensure that audio-visual media services provided by media service providers under their jurisdiction, which may be harmful to minors, are made available only subject to conditions that would ensure that minors will not be exposed to them. These measures include time of broadcast, age verification tools or other technical measures, determined to be in proportion to the potential harm of the material. It also requires that "personal data of minors collected or otherwise generated by media service providers pursuant to paragraph 1 shall not be processed for commercial purposes, such as direct marketing, profiling and behaviorally targeted advertising." Similar requirements are imposed on video sharing platform providers in Article 28b.

11 Regulation (EU) 2016/679 (General Data Protection Regulation) available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 and https://gdpr-info.eu.

12 Regulation Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, available at https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN.

13 Proposal a Regulation for laying down rules to prevent and combat child sexual abuse COM/2022/209 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472.

14 A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), p. 9, COM (2022) 212 Final, Brussels, 2020., available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN .

15 The General Data Protection Law (unofficial translation from Portuguese), https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.

16 Brazil LGPD Article 14

17 Brazil LGDP, Article 14, Section 5.

18 Brazil LGDP, Article 14, Section 4.

19 H.R.8152—American Data Privacy and Protection Act available at https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

20 Among the provisions that apply to children are a prohibition on targeted advertising to children and minors, data transfer requirements that apply to children and minors' data and establishing within the Federal Trade Commission a division dedicated to children's privacy. It also requires that the Inspector General submit a report to Congress on the effectiveness of the safe harbor provision of the Child Online Privacy Protection Act.

21 AB-2273 The California Age-Appropriate Design Code Act available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273.

22 House of Commons of Canada, Bill C-27 at Digital Charter Implementation Act, "Consumer Privacy Protection Act" at s. 1(2).

23 Ibid. at s. 4(a) and s. 55.

24 Quebec Act respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1, available at https://www.canlii.org/en/qc/laws/stat/rsq-c-p-39.1/latest/rsq-c-p-39.1.html, amended by the Act to modernize legislative provisions in regard to the protection of personal information, 2021, available https://www.canlii.org/en/qc/laws/astat/sq-2021-c-25/latest/sq-2021-c-25.htm l at s. 4.1.

25 Ibid. at s. 28.1.

26 General comment No. 25 (2021) on children's rights in relation to the digital environment available at https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

27 Artificial intelligence and privacy, and children's privacy, Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, United Nations General Assembly, Human Rights Council, Forty-sixth session, February 22-March 19, 2021, Agenda item 3, https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session46/Documents/A_HRC_46_37_Add.6_AdvanceUneditedVersion.docx .

28 In May 2019, UNICEF published Artificial Intelligence and Children's Rights, available at https://www.unicef.org/innovation/reports/memoAIchildrights ,a series of case studies that illustrate the ways in which artificial intelligence-based technologies affect children's human rights. It identifies opportunities to use artificial intelligence in ways that positively impact children's wellbeing, and highlights questions that researchers, corporations, governments, educators and parents should ask and address to better protect children from the negative consequences of AI. UNICEF's stated goal for the document is to help a range of stakeholders to better understand and lay a framework for addressing the potential impact of artificial intelligence on today's children, and on future generations.

29 UNICEF Children's online privacy and freedom of expression: Industry toolkit. 2018 available at https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

30 "Convention on the Rights of the Child," 20 November 1989, General Assembly resolution 44/25, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child. The CRC states that children have rights to privacy and freedom of expression. Article 16 states that "[n]o child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honor and reputation" and reaffirms that "the child has the right to the protection of the law against such interference or attacks". Article 13 states that children shall have the right to freedom of expression. Signatories to the convention include 194 countries.

31 The Toolkit, op. cit.,also proposes a checklist for use by companies whose activities have an impact on children's privacy and expression rights in a digital world, and offers considerations for online platforms, mobile operators and device manufacturers. The questions address the impact on children's privacy and freedom of expression across four activities in the digital environment: 1) obtaining children's personal data, 2) using and retaining children's personal data, 3) ensuring children's access to information, and 4) educating and informing children online.

32 Issues of children's privacy are often considered in association with concerns about content safety. Because they involve age verification, questions related to protecting children from harmful content and from online predation may be difficult to separate in considerations related to protecting children's online privacy.

33 Moreover, the Council of Europe notes that "personal data can be processed to the benefit of children, States should take measures to ensure that children's personal data is processed fairly, lawfully, accurately, and securely, for specific purposes and with the free, explicit, informed and unambiguous consent of the children and/or their parents, carer or legal representative, or in accordance with another legitimate basis laid down by law. The data minimization principle should be respected, meaning that the personal data processing should be adequate, relevant and not excessive in relation to the purposes for which they are processed." Recommendation CM (Rec 2018(7) of the Committee of Ministers to Member States on Guidelines to protect, defend and fulfil the rights of the child in the digital environment). Appendix to the Recommendations, No. 29, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016808b79f7.

34 For example, Hong Kong and Colombia establish the age of consent for data collection at 18, Japan at 15, Thailand at 20, and the US at 13. Perhaps even more challenging are the laws that require companies to engage in a subjective assessment of a child's capacity to make an informed decision about data collection when determining whether their consent will meet legal requirements.

35 For example, Argentina's data protection law does not expressly address data pertaining to minors and does not specify the circumstances when a minor's consent is considered valid, but relies on the National Civil and Commercial Code, which provides that minors (children under 18 years old) lack the capacity to exercise their rights and distinguishes between minors over and under the age of 13. However, guidance articulated by the data protection authority provides that whether minors may provide informed consent to the processing of their personal data depends on their capacity and level of development.

36 The variation in the age of consent and in consent requirements is illustrated in the table found in Appendix Four.

37 These challenges are further compounded by the need to comply with laws and regulations that address other aspects of children's online safety and well-being.

38 "Best interests of the child" is central to the analysis required by the UK ICO's Age-Appropriate Design Code, The Irish Data Protection Commissioner's Fundamentals for a Child Oriented Approach to Data Protection and other emerging guidance.

39 Moreover, introducing child-protective measures, no matter how well intentioned, may result in a two-tier level of service in which some children experience access only to an inferior experience, and thus risk depriving them of the ability to exercise the full range of rights as articulated in the United Nations' Convention.

40 Greater visibility from regulators about their expectations related to how these risks are to be managed when data about children is collected to protect them, i.e., for purposes of content moderation, would benefit companies' efforts in this regard.

41 Questions of consent to collection and processing of children's data in education settings and platforms raises its own issues of transparency, consent and appropriate use.

42 In the United States, for example, the Child Online Privacy Protection Act provides that children may provide consent at age 13. The GDPR sets that age at 16. In Korea, the PIPA establishes the age of consent at 14.

43 For example, Argentina's Personal Data Protection Law does not specifically provide for children's privacy. And does not specify under what circumstances the consent of a minor may be valid. However, other regulations not specifically related to personal data protection contain important rules that affect data protection. Article 52 and 1770 of the National Civil and Commercial Code (the Code) protect the right to privacy. Article 22 of Law No. 26.061 on the Protection of Girls, Boys and Adolescents protects minors' data. The Argentine data protection authority (AAIP) has issued detailed guidance about implementation and compliance with the PDPL. The AAIP established 'Guiding criteria and indicators of best practices in the application of the Act' (the AAIP Criteria) which correspond to the Code's criteria. The Code presumes that minors (children under 18 years old) lack the capacity to exercise their rights. However, it distinguishes between minors under and over 13 years of age. It establishes an irrebuttable presumption that children under 13 cannot perform "voluntary rightful acts," but children over 13 who are sufficiently mature can.

44 In some cases, depending on prevailing cultural norms, parents may be reluctant to be asked to consent on behalf of their teenagers and may view such an intervention as compromising their child's privacy or personal autonomy.

45 The feasibility of making such an assessment in practice is not clear. Moreover, even if checking such documentation in each individual case were feasible, it is not clear how an organization could ascertain that the documentation provided is valid and up-to-date (e.g., how could an organization be aware of instances when a parent has been deprived of parental rights by a court?).

46 Article 6 of the EU GDPR articulates several bases for the lawful processing of data. These include consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement and a public interest. In this section, we focus only on legitimate interests as a basis for the lawful processing of children's data given the unique challenges of that basis in the context of processing children's data.

47 The EU GDPR provides: "Processing shall be lawful only if and to the extent that at least one of the following applies: (1) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (2) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (3) processing is necessary for compliance with a legal obligation to which the controller is subject; (4) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and (6) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." Article 6(1). When deciding whether data may be processed based on a company's legitimate interests, Article 6 (3) sets forth five considerations that must be taken into account in making the determination.

48 A bill introduced in Sri Lanka, Act to Provide for the Regulation of Processing of Personal Data (July 2021) ('the Draft Bill'), available at https://www.parliament.lk/en/news-en/view/2501?category=6 , provides that data pertaining to children is considered sensitive and a "special category" of data. In paragraph (f) of Schedule I of the Draft Bill, the processing of personal data is lawful if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of the data subject which require protection of personal data, in particular where the data subject is a child. [Emphasis added]

49 Article 6 of the GDPR provides that processing may be lawful when it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

50 The Fundamentals emphasize this balancing test required of organizations as they determine whether legitimate interest may be relied upon as a legal basis to process children's data. It states that, "[t]he central condition for reliance on this legal basis is that the legitimate interests which are pursued by the organization (or the third party) are not overridden by the interests, rights, and/or fundamental freedoms of the data subject. This means that the organization needs to carry out a balancing exercise when assessing whether the processing of children's personal data should take place. Such a balancing test involves (1) identifying the legitimate interests of the controller or another person/organization which are sought to be achieved, (2) demonstrating why/how processing is a necessary and proportionate means to achieving the legitimate interests, and (3) balancing those legitimate interests against the child's interests or fundamental rights and freedoms." (emphasis added) Op. cit.

51 In this paper, we refer to the process of establishing whether a minor is of legal age to access online material or platform or participate in an online activity as age assurance. We distinguish this from age verification, because in many cases it is only important to know that a child's age is above or below that designated by a law, regulation or code (e.g., that they are over age 13), and it is not necessary to establish their age exactly (e.g., that they are age 14). We also make this distinction because the level of assurance required in many cases needs to be commensurate to the risks posed (e.g., it may be important to know with greater certainty that a teenager is over 18 before they are able to access pornography; it is arguably less of an issue when a site attempts to exclude children who may wish to purchase toys or games online). The ICO makes a similar distinction in its 2021 Opinion, in which it defines age verification as "determining a person's age with a high level of certainty by checking against trusted, verifiable records of data," and age estimation as "estimating a person's age, often by algorithmic means. Outputs vary from a binary determination as to whether someone is or is not an adult, through to placing an individual in an age category." 1.3, p. 5, Op cit.

52 The French Government has threatened to block five major pornographic websites, unless they introduce age verification to check users are over age 18. France's Higher Audiovisual Council gave the sites until December 28, 2021 to comply with the law https://www.csa.fr/Reguler/Espace-juridique/Les-textes-adoptes-par-l-Arcom/Les-decisions-du-CSA/Decision-du-13-decembre-2021-mettant-en-demeure-la-societe-MG-Freesites-Ltd-en-ce-qui-concerne-le-service-de-communication-au-public-en-ligne-Pornhub. A network of laws in Germany provides protections for minors. In March 2022, Germany's Commission for Youth Media Protection decided unanimously to impose a network ban on the most visited porn website in the country for failure to block underage users, in accordance with a new law requiring such sites verify the age of users.

53 This may not be feasible in practice for some types of services because currently mechanisms that allow an organization to have certainty about granular ages require collection of a disproportionate amount of information about all of their users. The Times UK, July 2021. "German Plan to Stop Under 18s Accessing Pornography," available at https://www.thetimes.co.uk/article/german-plan-age-stop-under-18s-accessing-pornography-w9xpdl9rm.

54 UNICEF highlights the need for this balancing, stating that, "Using age to determine children's exposure to risk online requires a balancing of children's rights against an assessment of the different risks to which they are exposed. All platforms and websites must take into account the ages set by data protection laws and industry age ratings, as well as the implications of age for other risks, such as sexual exploitation or exposure to harmful content." Digital Age Assurance Tools and Children's Rights Online Across the Globe, April 2021, available at https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf.

55 In some countries, the government agencies that collect and consolidate data about citizens could provide models for nation-wide age assurance solutions. For example, in Singapore Myinfo, a product provided under the National Digital Identity (NDI) Smart Nation Strategic National Project, helps citizens and residents manage and consent to have their personal data retrieved across participating Government agencies to pre-fill forms for digital transactions.

56 Layered assurance is a technique in which the age of an individual is assessed by more than one test or process. It provides multiple levels of assurance as required by the underlying transaction or activity. It should be noted that some jurisdictions have rejected the use of alternatives such as math problems and puzzles for this purpose.

57 It will be important, however, to manage the friction introduced by layered assurance so that it does not discourage individuals' use of new services.

58 For example, age assurance requirements at the sign-up stage of a user's engagement may need to be more rigorous than at later points when age has been established.

59 One provider of age assessment services has indicated that it trained its AI model with data about children whose parents had consented for images to be used as part of a program organized by the UK ICO. The company says its AI model cannot actually see "age," such as wrinkles or greying hair, but relies on the pixels that make up an image of someone, and which it can compare with its knowledge of millions of similar images it has been trained on before. The company asserts that the image is automatically deleted once the software estimates the person's age, with no human ever seeing the picture and no data stored. "AI spots underage app users at a glance," The Times UK, October 26, 2021. Also, the question of data storage may also be addressed by determining where age verification would best occur. When the verification technology and processing is confined to the device alone, concerns about data collection and potential storage and secondary may be significantly lessened.

60 In some instances, biometric data may not be used to identify a unique individual but rather only to determine whether they possess characteristics of persons in a particular age group.

61 Canada has recently proposed new legislation that would regulate the creation and use of artificial intelligence systems in an attempt to address some of these challenges. House of Commons of Canada, Bill C-27 at Digital Charter Implementation Act, the "Artificial Intelligence and Data Act" available at https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

62 An example of regulator review of age verification tools is Germany's Commission for the Protection of Minors in the Media's endorsement of three technologies that verify people's ages using AI to prevent minors' exposure to harmful content. "German Youth Protection Body endorses AI as an age verification tool," Euractiv, 1 June 2022, available at https://www.euractiv.com/section/digital/news/german-youth-protection-body-endorses-ai-as-biometric-age-verification-tool.

63 Companies that use profiles to target ads to children raise concerns about eliminating this practice. They note in particular that if ads are not targeted, children will see an increased number of irrelevant advertisements.

64 Practices like these are often referred to as "contextual" advertising. Contextual advertising becomes more complicated when carried out in social media, where the underlying content may not have a clearly defined "context."

65 In some cases, for example, profiling can help companies comply with laws that prohibit children from purchasing alcohol or accessing online pornography or gambling sites.

66 ICO, Age Appropriate Design Code, Provision 12, Profiling, available at https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/12-profiling/.

67 Age verification for this purpose also raises the question of whether the verification should be carried out by the platform or the vendor.

68 Irish Privacy Commissioner, Fundamentals, Section 6.1.3, page 54.

69 The Office of the Privacy Commissioner of Canada, "Privacy & Online Behavioral Advertising Guidelines," 2011, revised 2021, available at https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl_ba_1112/.

70 Article 5(1) of the EU's GDPR places emphasis on transparency, stating that "data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject." The GDPR also contains more specific provisions about the information that companies must provide to data subjects when processing their personal data.

71 EU GDPR, Articles 13 and 14.

72 "The controller shall take appropriate measures to provide any information referred to in Article 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject the information may be provided orally, provided that the identity of the data subject is proven by other means."

73 The UK Age Appropriate Design Code sets out five specific requirements for providing transparency about the collection and use of children's data: 1) Provide clear privacy information. 2) Provide 'bite-sized' explanations at the point at which use of personal data is activated. 3) Provide clear terms, policies, and community standards. 3) Present information in a child friendly way. 4) Tailor information to the age of the child. Pp. 38-40.

74 Ibid. pp. 40-42.

75 For example, Brazil's LGPD includes detailed requirements related to transparency, and specified how information about processing data should be made available. Op. cit. The law in China requires the data processor provide a privacy policy if it processes children's personal information. Canada's PIPEDA requires that companies post privacy notices and in guidance, reminds companies to make sure that young users can understand the explanation of data practices and risks. Op. cit. Colombia's data protection law requires that the informed consent of a parent or guardian must be obtained before processing minors' personal data. Op cit.

76 PIPEDA, s. 6.1. Guidance issued by the Office of the Privacy Commissioner of Canada indicates that parental consent is required where a child is unable to provide meaningful consent to personal information practices, which in all but exceptional cases, means that anyone under the age of 13. And, for minor children over the age of 13 to provide meaningful consent, the OPC indicates that consent will only be meaningful where the organization has developed and adapted their consent processes to take into consideration the maturity level of minors. Further, organizations that collect, use, and disclose minors' personal information are expected to be able to readily demonstrate on demand that their chosen process leads to meaningful and valid consent.

77 It is important to emphasize that a risk-based approach to children's privacy involves identifying, evaluating, and mitigating the risk data collection and processing raises for the child. While companies will likely have implemented processes to identify and address risks to brand and reputation and exposure to legal liability, protecting privacy on the basis of risk requires a shift in orientation from risk to the company to risk to the child.

78 CIPL will examine in detail the potential benefits and challenges of a risk-based approach, and how one might be designed to work, in Policy Paper II.

79 Artificial Intelligence Act (AIA) "Obligations of providers of high-risk AI systems Providers of high-risk AI systems shall: (e)ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;" Brussels, 21.4.2021, COM (2021) 206 final, 2021/0106(COD) available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN. Article 26 of the DSA available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0825&from=en.

80 Personal Data Protection Act 25.326 of 2000, available at http://www.jus.gob.ar/datos-personales/english-version/regulation/acts-and-decrees.aspx.

81 Proteccion de los datos personales Decreto 1558/2001 available (in Spanish) at http://www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf.

82 11.179 Law, Penal Code of the Argentine Nation, Section 157bis, Para. 1 available at https://observatoriolegislativocele.com/en/Criminal-Code-of-the-Argentine-Republic-Law-11179/.

83 Argentina Commercial Code, Article 12, available at https://ppp.worldbank.org/public-private-partnership/sites/ppp.worldbank.org/files/documents/Ley15.349(1946)_SP_0.pdf.

84 Resolution 4/2019, available (in Spanish) at http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318874/norma.htm.

85 The Privacy Act 1988, available at https://www.legislation.gov.au/Series/C2004A03712.

86 Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

87 Office of the Australian Information Commissioner, Australian Privacy Principles, Section B52-55, available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts.

88 Guidance of the Australian Government, Office of the Australian Information Commissioner, available at https://www.oaic.gov.au/privacy/your-privacy-rights/children-and-young-people.

89 Law 164/2011 available, in Spanish, at https://www.wipo.int/edocs/lexdocs/laws/es/bo/bo052es.pdf.

90 Law 453/2013 available, in Spanish, at https://wipolex.wipo.int/en/text/336463.

91 Supreme Decree No. 28168 of 2005 - Transparency in the Management of Executive Power (unofficial translation) https://www.rti-rating.org/wp-content/uploads/2018/09/Bolivia.RTI_.2005.informal-translation.pdf.

92 Law No. 548 of November 2018 (in Spanish) available at https://siteal.iiep.unesco.org/sites/default/files/sit_accion_files/siteal_bolivia_0248.pdf.

93 Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019).

94 Brazil LGPD, Article 14 (1).

95 Law No. 8.069 of 13 July 1990, art. 2.

96 Brazil LGPD, Article 14 (1). The Brazil LGPD may be considered to adopt a higher protective standard if compared to the US Children's Online Privacy Protection Rule, which is aimed to the "operators of websites and online services" in regulating what must be done to "protect children's privacy and safety online," as specified in the FTC website, or to the EU General Data Protection Regulation, which states "conditions applicable to a child's consent, in relation to information society services" in Article 8).

97 Brazil LGPD, Article 14 (5).

98 Brazil LGPD, Article 14 (3).

99 Brazil LGPD, Article 14 (4).

100 Brazil LGPD, Article 14 (6).

101 British Columbia Personal Data Protection Act, SBC 2003, c 63, available at https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01.

102 Alberta Personal Information Protection Act, SBA 2003 c P-6.5, available at https://www.canlii.org/en/ab/laws/stat/sa-2003-c-p-6.5/latest/sa-2003-c-p-6.5.html.

103 Quebec Act respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1, available at https://www.canlii.org/en/qc/laws/stat/rsq-c-p-39.1/latest/rsq-c-p-39.1.html, amended by Bill 64, an Act to modernize legislative provisions in regarding to the protection of personal information, 2021, http://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html.

104 See the Office of the Privacy Commissioner of Canada's Guidelines for obtaining meaningful consent available at https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805.

105 Ibid. at Chapter 9.53.1.

106 Available at http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

107 This definition of a minor is consistent with the definition under the national "Information Security Technology—Personal Information Security Specification."

108 Colombia Statutory Law 1266 of 2008, available at https://www.hlbcolombia.com/legal/?lang=en

109 Ley 1581 de 2012 available at https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

110 The protection of personal data is a constitutional and fundamental right in Colombia. Article 15 of the Colombian Political Constitution (the Constitution), available at https://www.corteconstitucional.gov.co/english/Constitucio%CC%81n%20en%20Ingle%CC%81s.pdf demands that, when personal data is collected, processed or transmitted, guarantees provided in the Constitution must be respected.

111 Title 3, Article 7.

112 Colombia Decree 1377 of 2013, available (in Spanish) at https://www.littler.com/files/press/related-files/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013%20(2)%20(2).

113 Law No. 151 of 2020, available at https://www.acc.com/sites/default/files/program-materials/upload/Data%20Protection%20Law%20-%20Egypt%20-%20EN%20-%20MBH.PDF.

114 Egypt's Child Law No. 12 of 1996, Part 1 Article 2(2), available at https://www.refworld.org/docid/5a4cb6064.html.

115 Ibid., Article 12.

116 Regulation (EU) 2016/679,

117 Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, p. 11, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136.

118 Article 4 (25) of the EU's GDPR defines 'information society service' in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council [19]; The Directive Article 1(1)(b) defines "information society service" as 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. The definition provides further specificity about the meaning of "at a distance," "by electronic means," and "at the individual request of a recipient of services."

119 GDPR Article 8(1).

120 GDPR Article 8(2).

121 GDPR Article 12(1) provides: The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

122 GDPR Article 40(2)(g).

123 GDPR Article 41(1).

124 It should be noted that the EU also is adopting the Digital Markets Act (DMA) and the Digital Services Act (DSA).

The DMA only refers generally to children, stating that: "[c]hildren merit specific protection with regard to their personal data, in particular as regards the use of their personal data for the purposes of commercial communication or creating user profiles. The protection of children online is an important objective of the Union and should be reflected in the relevant EU law. [In this context, due regard should be given to the DSA]. Nothing in this Regulation exempts gatekeepers from their obligations concerning protection of children laid down in applicable EU law."

The DSA focuses on content moderation on digital platforms, and the need to address "wider societal concerns stemming from the way online platforms shape information flows," including online advertising. Platforms accessible to minors would be required to implement specific measures to protect them, including full bans on targeted advertising. It should be noted that small and medium-sized enterprises are excluded from the scope of the DSA.

125 GDPR Article 8.

126 GDPR Article 8(1).

127 France and Greece have set the age of consent at 15; Spain establishes that minors are children under the age of 14; Denmark, Portugal, Sweden and the UK allow for consent at age 13.

128 The law in Germany is further complicated by its youth protection laws, which require that all online service providers must generally ensure that minors cannot access any content that is deemed harmful for their respective age group. German law offers online service providers a choice of three possible means to comply with this obligation:

Use scheduling restrictions to ensure that harmful content is not available during daytime, i.e., when minors would usually be online.

Employ technical measures to ensure that minors are at least significantly impeded (if not fully blocked) from accessing any content that is not suitable for their age group.

Tag content with age labelling in a format that officially approved youth protection software can read.

In March 2021, Germany took the further step of enacting legislation intended to reform youth protections in the media. The new regulations provide for the participation of children and young people, one of the basic principles of the UN Convention on the Rights of the Child. The law obliges platform providers to take precautionary measures to counter the risks of children accessing inappropriate content. These measures include child-friendly terms and conditions, safe default settings for the use of services that limit the risks of use depending on age, for example, by ensuring that user profiles cannot be found by search engines, and easy-to-find information on provider-independent advice, help and reporting mechanisms. Support in this regard can be provided by voluntary self-regulation organizations. Together with service providers, self-regulatory organizations are encouraged to articulate guidelines for the implementation of safety measures and take into consideration the views of children and young people in their development.

129 These variations in law are further nuanced by guidelines published by Member State authorities, discussed later in this paper and the European Commission's release of its report on A Better Internet for Kids, discussed later in this paper.

130 The Data Protection Act, 2012 (ACT 843) available at https://www.dataprotection.org.gh/data-protection/data-protection-acts-2012.

131 Ibid., Article 37(1)(a).

132 The Children's Act 1998, Part I Subpart, Section 1, available at https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/56216/101251/F514833765/GHA56216.pdf.

133 The Personal Data Privacy Ordinance (Cap. 486), available at https://www.elegislation.gov.hk/hk/cap486.

134 The six data protection principles address (1) data collection, (2) accuracy and retention, (3) data use, (4) data security, (5) openness, and data access and correction. Officer of the Privacy Commissioner for Personal Data, Hong Kong, available at https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html.

135 The Personal Data (Privacy) (Amendment) Ordinance, Ord. No. 32 of 2021, available at https://www.gld.gov.hk/egazette/pdf/20212540/es12021254032.pdf.

136 The Personal Data Privacy Ordinance, Op Cit., fn. 54, Section 2(1).

137 "Collection and Use of Personal Data through the Internet—Points to Note for Data Users Targeting at Children," Office of the Privacy Commissioner for Hong Kong, December 2015, available at https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_children_e.pdf.

138 "PCPD Provides Guidelines on Children's Privacy during the Pandemic," April 2, 2022, available at https://www.pcpd.org.hk/english/news_events/media_statements/press_20200402.html.

139 Several Indian laws are drafted with an intention to protect children from abuse and obscenity, among others. These include the Penal Code 1860; the Information Technology Act 2000 and the Protection of Children from Sexual Offenses Act 2012. India's Personal Data Protection Bill, intended to provide a comprehensive framework for personal data and which included provisions specific to protection of children's data, was withdrawn from consideration by the legislature in August 2022. "India Withdraws a Proposed Law on Data Protection," The New York Times, August 4, 2022, available at https://www.nytimes.com/2022/08/04/business/india-data-privacy.html.

140 National Policy for Children 2013, available at https://wcd.nic.in/sites/default/files/npcenglish08072013_0.pdf.

141 Department of School Education and Literacy Ministry of Human Resource Development Government of India 2012, "National Policy of Information and Communications Technology in Schools 2012," available at https://planipolis.iiep.unesco.org/sites/default/files/ressources/india_national_policy_ict_education_2012.pdf.

142 Protection of Privacy Law, 5741-1981, unofficial translation found at https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf.

143 Basic Law: Human Dignity and Liberty, 5752-1992, found at https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/39134/97918/F1548030279/ISR39134.pdf.

144 Act on the Protection of Personal Information (Act No. 57 of 2003) available at https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

145 Ibid., Chapter IV.

146 In Japanese only, available at https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf.

147 Personal Information Protection Commission available at https://www.ppc.go.jp/en/.

148 Personal data protection act 2010 As at 15 June 2016 available at https://ilo.org/dyn/natlex/docs/ELECTRONIC/89542/102901/F1991107148/MYS89542%202016.pdf.

149 Personal Data Protection Regulations 2013, https://wcd.nic.in/sites/default/files/npcenglish08072013_0.pdf.

150 Child Act No. 611, 2001, Part I Section (2)(1), available at https://www.ilo.org/dyn/natlex/docs/WEBTEXT/65516/65279/E01MYS01.htm.

151 The CMA Code applies to data users that are licensees under the CMA. This includes (1) network facilities providers, (2) network services providers, (3) applications service providers, and (4) content applications service providers as defined under the CMA available at https://www.pdp.gov.my/jpdpv2/assets/2019/09/Communications-Sector-PDPA-COP.pdf Part I Section 3.2.

152 Privacy Act 2020, Public Act 2020 No 31 available at https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html.

153 Ibid., Information Privacy Principle 4.

154 Website of the New Zealand Privacy Commissioner, available at https://privacy.org.nz/tools/knowledge-base/view/2.

155 Constitution of the Russian Federation, Articles 23 and 24, available at http://archive.government.ru/eng/gov/base/54.html.

156 Council of Europe, European Treaty Series 108, Strasbourg 28.1.1981 available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

157 The Protection of Personal Information Act, 2013, available at https://popia.co.za.

158 Ibid., Section 34.

159 Ibid., Section 35.

160 Ibid., Sections 57-58.

161 The Personal Information Protection Act 2011 (Amended 2020) available at https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3.

162 Ibid., Section 1, Article 22 (6).

163 Ibid.

164 Ibid., Article 39.3 (4).

165 Personal Data Protection Act (No. 26 of 2012), available at https://sso.agc.gov.sg/Act/PDPA2012.

166 Ibid., Part 4, Division 1.

167 Available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-PDPA-for-Selected-Topics-310322.ashx?la=en.

168 "Advisory Guidelines on the Personal Data Protection Act for Selected Topics," Section 8.10, Personal Data Protection Commission Singapore, available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-17-May-2022.ashx?la=en.

169 Ibid., Section 8.4.

170 Ibid., Section 8.6.

171 Data Privacy Act of 2012 (Republic Act No. 10173), available at https://www.privacy.gov.ph/data-privacy-act/.

172 Available at https://www.privacy.gov.ph/data-privacy-act/.

173 Available at https://www.officialgazette.gov.ph/images/uploads/20160825-IRR-RA-10173-data-privacy.pdf.

174 In NPC Advisory Opinion No. 2017-49, involving teachers' right to search a minor student's mobile phone and NPC Advisory Opinion No. 2019-46, which dealt with an inter-agency council against trafficking (IACAT) request for information with the Philippine Statistics Authority (PSA), the NPC explained that a minor cannot validly provide the consent required by the Data Privacy Act.

175 Personal Data Protection Act, available at https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021.

176 Enforcement Rules of the Personal Data Protection Act, available at https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050022.

177 Civil Code, available at https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=B0000001.

178 Ibid., Chapter 2, Section 1, Article 13.

179 Available at https://library.siam-legal.com/thai-civil-and-commercial-code/.

180 Viet Nam Civil Code available at https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=45459

181 Decree No. 53/2022/ND-CP ("Decree 53/2022") available at https://www.pwc.com/vn/en/publications/2022/220908-pwc-vietnam-legal-newsbrief-decree-53.pdf

182 Law No. 51/2005/QH11 available at https://www.wto.org/english/thewto_e/acc_e/vnm_e/wtaccvnm43_leg_5.pdf

183 Vietnam: Amending the Telecoms Law, available at https://www.lexology.com/library/detail.aspx?g=e89c5367-e53b-41d6-b8f8-96fddb57d540

184 The Law on Children 102/2016/QH13 (5 April 2016), available at https://www.economica.vn/Content/files/LAW%20%26%20REG/102_2016_QH13%20Law%20on%20Children.pdf.

185 Ibid., Article 6.11.

186 Cybersecurity Law 2018, Article 29, available at https://www.economica.vn/Content/files/LAW%20%26%20REG/Law%20on%20Cyber%20Security%202018.pdf.

187 Ibid.

188 The UK GDPR is the retained EU law version of the General Data Protection Regulation (EU) 2016/679) (EU GDPR) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (SI 2019/419).

189 Article 17(1)(f) of the UK GDPR.

190 Ibid., Article 35.

191 Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when4.

192 Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/.

193 Ibid.

194 Examples include, The Health Insurance Portability and Accountability Act (HIPPA), available at https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf; US Public Law 104-191, the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., available at https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf, among others.

195 The Child Online Privacy Protection Act, Title 16, Chapter 1, Subchapter 1, Part 312, available at https://www.ecfr.gov/current/title-16/part-312.

196 COPPA does not apply to data about children collected online from parents or other adults.

197 Ibid., Part 312.2.

198 Ibid., Part 312.4, 312.5.

199 Ibid., Part 312.6.

200 Ibid., Section 312.11. COPPA also sets out specific requirements when modifications are made to the programs and grounds for revocation.

201 Privacy Rights for California Minors in the Digital World, Business and Professions Code [22580-22582], Division 8, Special Business Regulations [18400-22949.51, Chapter 22.1], available at https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=22580&lawCode=BPC.

202 The California Age Appropriate Design Code Act is discussed in this paper.

203 The Delaware Code, Section 6, available at https://delcode.delaware.gov/title6/c012c/index.html.

204 Codes and guidance on the issue of children's privacy, and on the broader question of children's safety and well-being online continue to proliferate. A comprehensive review of these is beyond the scope of this paper, and the discussion in this document is of necessity limited and intended to be illustrative. Recently released codes and guidance include, but are not limited to, The Dutch Code for Children's Rights, available at https://codevoorkinderrechten.nl/wp-content/uploads/2022/02/Code-voor-Kinderrechten-EN.pdf; Sweden's The Rights of Children and Young People on Digital Platforms, available at https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf; Denmark in April 2021 confirmed its commitment to protecting children's privacy and announced it was considering a standard, available at https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/apr/boern-og-unge-har-krav-paa-saerlig-beskyttelse, after the release of a report available at (available only in Danish) https://dataethics.eu/wp-content/uploads/gametech-marts-2021.pdf.

In addition, the EU Consent Consortium, a European Commission funded project to develop an EU-wide computer network for completing online age verification and securing parental consent when younger children wish to share personal data, state on its websites five core principles related to children's well-being and participation online, available at https://euconsent.eu. Finally, Singapore's Minister of Communications and Information, Josephine Tao, announced on March 4, 2022, that the government would release codes of practice to promote a safer online environment. The new codes would require online platforms to have in place systems to minimize the exposure of children and young people to harmful content, including content filters for child accounts, as well as mechanisms for parents to supervise and guide their children online.

205 Age Appropriate Design Code UK Information Commissioner's Office, available at https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/.

206 With respect to enforcement of the Code, the ICO states: "We will monitor conformance to this code through a series of proactive audits, will consider complaints, and take appropriate action to enforce the underlying data protection standards, subject to applicable law and in line with our Regulatory Action Policy. To ensure proportionate and effective regulation we will target our most significant powers, focusing on organizations and individuals suspected of repeated or willful misconduct or serious failure to comply with the law. If you do not follow this code, you may find it difficult to demonstrate that your processing is fair and complies with the [UK] GDPR or PECR (Privacy and Electronic Communications Regulations. We have various powers to take action for a breach of the [UK] GDPR or PECR, including where a child's personal data has been processed in breach of relevant provisions of these laws. This includes the power to issue warnings, reprimands, stop-now orders and fines." UK ICO https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/enforcement-of-this-code/.

207 Op. cit., fn. 93, page 24.

208 Reliance upon default settings for privacy as an alternative to consent is a question deserving of consideration. Care must be taken to ensure that default protections do not inadvertently downgrade the experience of children by enticing them to visit sites or access materials they are not yet ready for or prompt them to migrate to services that do not provide appropriate protections.

209 "Opinion on Age Assurance," available at https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf.

210 Fundamentals for a Child-Oriented Approach to Data Processing, Data Protection Commissioner of Ireland, December 2021, available at https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf.

211 Ibid., Commissioner's Forward.

212 The Fundamental that companies "know their audience" highlights an inherent tension that exists in addressing children's privacy—that the measures necessary to assure that a child is of an appropriate age to consent to data collection and processing also require the use of data about them.

213 Ibid., Section 5.7

214 The Digital Rights of Children, The CNIL, August 2021, available at https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online.

215 Ibid.

216 Ibid.

About the Centre for Information Policy Leadership

CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 90 member organisations that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at **http://www.informationpolicycentre.com/.**