



INDUSTRY TOOLKIT

CHILDREN'S ONLINE PRIVACY AND FREEDOM OF EXPRESSION



Acknowledgements

This Toolkit was developed by Carly Nyst, independent expert and consultant, and Amaya Gorostiaga and Patrick Geary from the UNICEF Child Rights and Business Unit. The Toolkit also benefitted from the inputs of a wide range of stakeholders in the public and private sectors, civil society and academia.

Design and Layout: Kathleen Morf

Copyright and Disclaimer

All rights to this guide remain with the United Nations Children's Fund (UNICEF). No part of this document may be replicated or redistributed without the prior written permission of UNICEF.

A reference to a non-UNICEF website does not imply endorsement by UNICEF of the accuracy of the information contained therein or of the views expressed.

May 2018 © United Nations Children's Fund (UNICEF) 2018

Contents

- INTRODUCTION** 4

- GENERAL PRINCIPLES ON CHILDREN’S ONLINE PRIVACY AND FREEDOM OF EXPRESSION**..... 6
 - Principle 1** Children have the right to privacy and the protection of their personal data 8
 - Principle 2:** Children have the right to freedom of expression and access to information from a diversity of sources 9
 - Principle 3:** Children have the right not to be subjected to attacks on their reputation 9
 - Principle 4:** Children’s privacy and freedom of expression should be protected and respected in accordance with their evolving capacities10
 - Principle 5:** Children have the right to access remedies for violations and abuses of their rights to privacy and free expression, and for attacks on their reputation10
 - Examples of practical implications 11

- CHECKLIST FOR COMPANIES ON CHILDREN’S ONLINE PRIVACY AND FREEDOM OF EXPRESSION** 12
 - 1:** Obtaining Children’s Personal Data 14
 - 2:** Using and Retaining Children’s Personal Data 18
 - 3:** Ensuring Children’s Access to Information 21
 - 4:** Educating and Informing Children Online 24

Introduction

More children around the world are spending more time, in more ways, online. While technology and digital media affect all aspects of children's lives, the policy debate to date has been largely shaped by the imperative to protect children from violence, exploitation and harmful content. This focus remains essential, yet may also risk overlooking how children exercise their full range of rights online, including their rights to privacy and freedom of expression. Against this backdrop, it is important to consider how children's rights to privacy and freedom of expression – as recognized in the United Nations Convention on the Rights of the Child (CRC) – are realized in a digital world.¹

Just as with adults, going online can put children's right to privacy at greater risk of intrusion. Public authorities may follow children's digital footsteps; businesses may collect and monetize children's data; and parents may publish children's images and information. Children are also more vulnerable to intrusions into their privacy as their capacity to understand the long-term impacts of sharing personal data is still developing. The fact that children's data can now be collected from the moment of their birth, the sheer volume of digital information that is generated during the first 18 years of life, and the multiple and advancing technological means for processing children's data all raise serious questions about how children's right to privacy can best be preserved and protected.

Freedom of expression and the right to information are fundamental to democracy, and children have embraced the Internet as a means to learn, share and participate in civic life. The Internet gives children instantaneous access to huge quantities of beneficial content, and offers a uniquely participatory pathway to empowerment. Even well-intended measures to prevent children from being exposed to potentially harmful messages or materials, such as parental controls, may in some circumstances end up hindering children's development into skilled, confident and responsible digital citizens.²

While governments have the primary obligation under international law to protect children's rights to privacy and freedom of expression online, the United Nations has also adopted Guiding Principles on Business and Human Rights that avow a corporate responsibility to respect human rights.³ This responsibility applies online as well as offline, for all groups, and across all rights. More specifically, the United Nations Special Rapporteur on the right to privacy has noted that "an increasing number of corporations today already gather much more personal data than most governments ever can or will",⁴ and the United Nations Special Rapporteur on the right to freedom of expression has recognized that "private industry ... wields enormous power over the digital space acting as a gateway for information and an intermediary for expression".⁵

¹ The CRC makes clear that children have specific 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 honour and reputation", and reaffirms that "the child has the right to the protection of the law against such interference or attacks". Building on the general principle that children have the right to participate in all aspects of their lives as articulated in Article 12, Article 13 states that children "shall have the right to freedom of expression ... includ[ing] freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice". Article 15 further recognizes "the rights of the child to freedom of association and to peaceful assembly", and Article 17 adds that children should "ha[ve] access to information and material from a diversity of national and international sources, especially those aimed at the promotion of [their] social, spiritual and moral well-being and physical and mental health."

² Some research has cast doubt on the effectiveness of parental controls. See, e.g., Oxford Internet Institute, Study casts doubt on whether internet filters in the home protect teenagers online, 14 March 2017, available at <www.oii.ox.ac.uk/news/releases/study-casts-doubt-on-whether-internet-filters-in-the-home-protect-teenagers-online>.

³ Guiding Principles for Business and Human Rights: Implementing the United Nations 'Protect Respect and Remedy' Framework, available at <www.ohchr.org/Documents/PublicationsGuidingPrinciplesBusinessHR_EN.pdf>.

⁴ Statement of the Special Rapporteur on the right to privacy, 9 March 2016, available at <www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21248&LangID=E>.

⁵ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 11 May 2016, A/HRC/32/38 at para [1].

The Guidelines for Industry on Child Online Protection, published by UNICEF and the International Telecommunications Union in 2015, further explore the corporate responsibility to respect children's rights in a digital world.⁶ This Toolkit builds on these Guidelines, expanding the consideration of children's rights to privacy and freedom of expression. It identifies five overarching principles, based in international human rights law, that should ground and shape decisions about children online.

These General Principles may be translated into practical action through the Checklist that follows,

which offers questions and recommendations for companies to assess how children's privacy and expression rights are considered across their websites, platforms, products, services and applications. The General Principles and Checklist were developed by UNICEF in consultation with a diverse range of stakeholders from the public and private sectors, academia and civil society. UNICEF continues to advocate for the full realization of children's rights, including the rights to privacy and freedom of expression. It is hoped that this Toolkit prompts greater respect for children's rights in a digital world.

⁶ Guidelines for Industry on Child Online Protection, available at <www.itu.int/pub/S-GEN-COP.IND-2013>.

GENERAL PRINCIPLES ON CHILDREN'S ONLINE PRIVACY AND FREEDOM OF EXPRESSION



General principles

There is a shared responsibility to protect, respect and realize the rights of the child, which in international law means a person under the age of 18.⁷ Thus, governments, businesses, parents, educators and children all have a role to play in advancing children's privacy and freedom of expression in a digital world. Guided by the best interests of the child,⁸ public obligations and private responsibilities should be governed by a set of general principles that put children's online privacy and expression rights in context:



1. Children have the right to privacy and the protection of their personal data.



2. Children have the right to freedom of expression and access to information from a diversity of sources.



3. Children have the right not to be subjected to attacks on their reputation.



4. Children's privacy and freedom of expression should be protected and respected in accordance with their evolving capacities.



5. Children have the right to access remedies for violations and abuses of their rights to privacy and free expression, and attacks on their reputation.

⁷ Article 1 of the CRC defines children as all persons under the age of 18 unless stated otherwise under national law.

⁸ CRC, Article 3.

General principles

PRINCIPLE 1:

Children have the right to privacy and the protection of their personal data.



Children’s right to privacy is multifaceted, and the physical, communications, informational and decisional aspects of children’s privacy are all relevant in the digital world. Children’s physical privacy is affected by technologies that track, monitor and broadcast children’s live images, behaviour or locations. Children’s communications privacy is threatened where their posts, chats, messages or calls are intercepted by governments or other actors, and children’s informational privacy can be put at risk when children’s personal data are collected, stored or processed. Children’s decisional privacy may be affected by measures that restrict access to beneficial information, inhibiting children’s ability to make independent decisions in line with their developing capacities.

In general, children’s privacy is more likely to be respected in a digital environment where:

- Children can privately and securely access information online
- Children’s communications and personal data are sufficiently protected from unauthorized access or intrusion
- Children’s privacy is considered in the design of websites, platforms, products, services and applications designed for, targeted at or used by children
- Children enjoy protection from online profiling

Going online has specific implications for children’s informational privacy, which is best protected where:⁹

- Children, or their parents or guardians, are required to provide their free and informed consent for the processing of their personal data¹⁰
- Children’s data are processed in a manner that is fair, lawful and transparent, and compatible with the purpose for which the data were obtained
- Children’s data are kept to what is minimally necessary, and are accurate and up to date
- Children are educated, informed and empowered to protect their personal data

⁹ Informational privacy principles are enshrined in the 1980 Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and echoed in the United Nations’ Human Rights Committee 1989 General Comment No. 16, the EU General Data Protection Regulation, and the United States Federal Trade Commission’s Fair Information Practice Principles.

¹⁰ Although other legal bases for data processing may exist, obtaining free and informed consent is the approach most consistent with children’s rights.

PRINCIPLE 2:

Children have the right to freedom of expression and access to information diversity from a diversity of sources.



The Internet provides tremendous opportunities for children to express themselves and presents children with a vast quantity of information at their fingertips, yet certain barriers prevent all children from enjoying these benefits equally. At the same time, while children may need assistance to safely exercise their rights to freedom of expression and access to information, protective measures may become unduly restrictive as children's capacities to navigate the digital world develop. Children are best able to exercise their rights to freedom of expression and access to information online where:

- Children have reliable and affordable access to digital technology, accounting for differences in language, literacy and capacity
- Children can freely and confidently use technology without disproportionate monitoring by governments or parents, unnecessarily strict moderation or policing of user-generated content, or unwarranted limitations on anonymity
- Children can explore the digital world without encountering overly restrictive filters, whether at a network or device level, or other systems or mechanisms that restrict access to potentially beneficial content
- Children can access information from a diversity of sources that is adapted to their interests and levels of understanding, noting that requirements to provide payment or supply personal data may act as a barrier to accessing online content

PRINCIPLE 3:

Children have the right not to be subjected to attacks on their reputation.



Children's reputations are increasingly shaped by the growing quantities of information available about them online. This not only influences children's interpersonal relationships, but may also have an impact on their ability to access services and employment as they enter adulthood. While the extent, nature and importance of reputation continue to evolve in a digital world, children may be empowered to protect their online reputation where:

- Children can easily request that their personal data are corrected or deleted, especially where the data have been collected or published without their permission, and can seek the removal of content they believe is damaging to their reputation
- Parents or guardians, media outlets and other third parties refrain from sharing information that could undermine children's current or future reputation
- Children are equipped with digital literacy skills that enable them to make informed choices about generating and sharing personal content
- Parents or guardians are equipped to guide and assist their children in taking appropriate action to protect their online reputation

PRINCIPLE 4:

Children's privacy and freedom of expression should be protected and respected in accordance with their evolving capacities.



Childhood is a continuous and rapid period of development, and no single approach can fully guide efforts to realize children's rights to privacy and freedom of expression. Rather, children's rights in a digital world must be considered in light of their evolving capacities, with children becoming more able to exercise their rights online as they grow and mature. Among other things, acknowledging children's evolving capacities may mean that:

- Children, in accordance with their age and maturity, require assistance to understand and engage with the terms and conditions for using a website, platform, product, service or application
- Children are not asked to provide informed consent for the collection and processing of their personal data when they do not possess the capacity to do so
- Parents or guardians play a more active role in deciding the scope and nature of the information and content that younger children can share and consume, while also considering children's views and opinions
- Parental controls and other monitoring and filtering tools take account of older children's rights and abilities to make empowered and informed decisions online

PRINCIPLE 5:

Children have the right to access remedies for violations and abuses of their rights to privacy and free expression, and for attacks on their reputation.








All children have the right to seek an effective remedy where their rights have been violated or abused.¹¹ Given the global and connected nature of the Internet, it can be complex to realize children's right to remedy in a digital world. To seek a remedy, children must first understand that they have rights, that these rights are exercised online, and that they have the right to complain when these rights are not respected. Accordingly, children, or their parents and guardians, will be most able to seek remedies where:

- Children are informed about their rights to privacy and freedom of expression, and understand how these rights are affected by actions such as data collection, filtering and content moderation
- Children can easily access transparent reporting mechanisms that are adapted for their levels of digital literacy and understanding, bearing in mind their age, maturity and evolving capacities
- Children, or their parents or guardians, can file complaints or report content in a way that covers the full range of their privacy and expression rights
- Children receive expeditious responses to any complaints filed, including explanations of decisions made and avenues to seek further review or redress

¹¹ See Committee on the Rights of the Child, General Comment no. 5; Human Rights Committee, General Comment No. 5; United Nations Human Rights Council, Resolution on the Rights of the Child: Access to justice, A/HRC/25/L.10, 25 March 2014.

EXAMPLES OF PRACTICAL IMPLICATIONS

Children’s rights to privacy and freedom of expression are affected by a diverse and growing array of issues, concerns, mechanisms and practices in the digital world. Translating the General Principles on Children’s Online Privacy and Freedom of Expression into action demands an understanding of the links between systems and actions in the online environment and children’s privacy and expression rights. While far from exhaustive, the list below provides some examples that have an impact on children’s rights online.

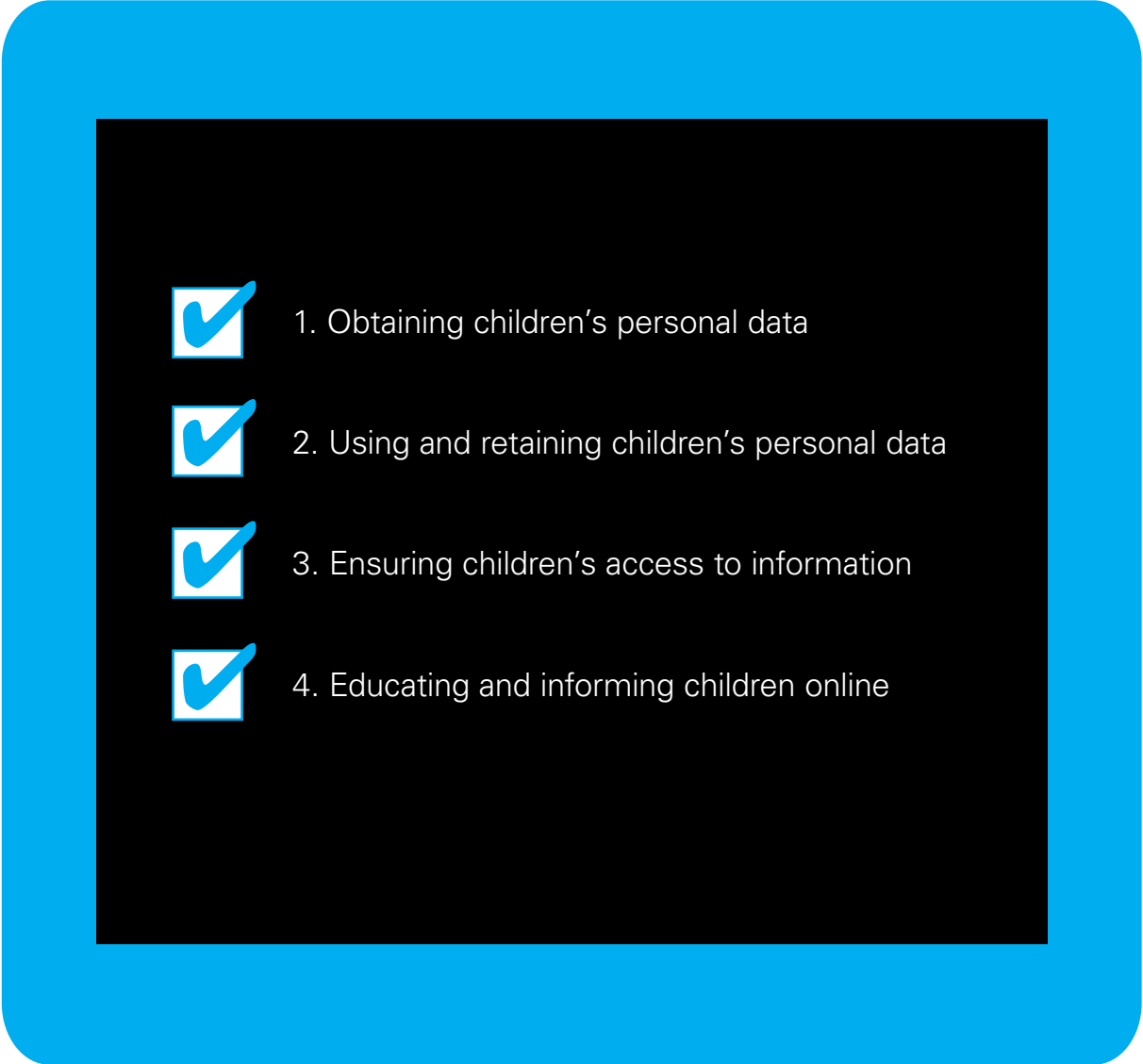

PRINCIPLE	AFFECTED BY
 <p>1. RIGHT TO PRIVACY AND PROTECTION OF PERSONAL DATA</p>	<ul style="list-style-type: none"> • Monitoring technologies • Surveillance • Data collection, analysis and retention • Profiling
 <p>2. RIGHT TO FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION</p>	<ul style="list-style-type: none"> • Barriers to accessing the Internet, including cost and literacy • Content moderation • Network or device-level filtering • Prohibitions on pseudonyms • Data collection requirements for accessing content
 <p>3. RIGHT TO PROTECTION OF REPUTATION</p>	<ul style="list-style-type: none"> • Digital literacy • Complaints mechanisms for content or data removal • Sharing of children’s personal information without consent
 <p>4. RIGHTS PROTECTED IN ACCORDANCE WITH EVOLVING CAPACITIES</p>	<ul style="list-style-type: none"> • Capacity to give informed consent • Ability to understand terms of service • Parental monitoring and decision-making
 <p>5. RIGHT TO ACCESS A REMEDY</p>	<ul style="list-style-type: none"> • Transparent reporting on human rights impacts • Human rights education • Accessible and effective reporting tools

CHECKLIST FOR COMPANIES ON CHILDREN'S ONLINE PRIVACY AND FREEDOM OF EXPRESSION



Checklist for companies

This Checklist is designed for use by any company that has an impact on children's privacy and expression rights in a digital world. It contains questions that are generally applicable across the digital environment, and offers additional considerations for online platforms, mobile operators and device manufacturers. Companies can use the Checklist to initiate a standalone review of policies and practices, or as a means to integrate child rights considerations into existing and regular assessments. The Checklist groups potential impacts on children's privacy and freedom of expression into four categories:

- 
1. Obtaining children's personal data
 2. Using and retaining children's personal data
 3. Ensuring children's access to information
 4. Educating and informing children online
- 

1 OBTAINING CHILDREN'S PERSONAL DATA

Respecting children's rights to privacy and the protection of personal data in the context of the Internet and digital technologies means, first and foremost, that companies have a legitimate basis for processing children's personal data and do so in a fair and lawful manner. Children's privacy is best protected where children provide free and informed consent for the processing of their personal data or, where they lack the capacity to do so, parents or guardians provide this consent on children's behalf. Children's right to privacy should be considered in the design of websites, platforms, products, services and applications, including devices and toys, and with regard to default privacy settings.

GENERAL QUESTIONS FOR CONSIDERATION	CONTEXT
<input type="checkbox"/> Does your company process the personal data of children under the age of 18?	Children's personal data merit specific protection, especially when the data are collected and processed to develop profiles or for marketing, or when a service or application is directed towards children. ¹²
<input type="checkbox"/> Does your company seek consent from children under the age of 18 to process their personal data? If so, how does your company ensure that this consent is freely given, specific, informed and unambiguous?	For children's consent to be meaningful, it must be sought in a manner and form that matches their level of understanding. To seek children's meaningful consent, companies must communicate in plain language and can use innovative techniques, such as diagrams, images and videos, to explain to children how their personal data would be handled. Under European law, consent should be freely given, specific, informed and unambiguous, and requires a clear, affirmative act to authorize the processing of personal data. ¹³
<input type="checkbox"/> Does your company set an age threshold below which you require parents or guardians to provide informed consent for the processing of children's personal data? If so, below what age is parental consent required?	<p>Requesting consent for data processing gives children control over how their personal information is used and shared, and empowers children to understand and exercise their right to privacy. Under European law, consent must be sought for data processing unless there is another permissible reason to process personal data.¹⁴ Although there are other legal bases for processing data, obtaining children's consent increases the likelihood that children are aware of the processing of their personal data and empowered to exercise their rights.</p> <p>Given children's evolving capacities, parents or guardians may in some instances be better placed than children to authorize the processing of children's personal data. Accordingly, laws in many jurisdictions recognize that children below a certain age are often unable to give informed consent, because they are unlikely to understand the implications of providing personal data. Under U.S. law,¹⁵ parental consent is required for the processing of personal data on sites directed to children under the age of 13, or where companies have actual knowledge that a child under 13 is using their service. Similarly, European law requires all Member States to set an age of consent for data processing between ages 13 and 16.¹⁶</p>

GENERAL QUESTIONS FOR CONSIDERATION	CONTEXT
<input type="checkbox"/> If your company relies on parental consent for processing children’s personal data, how does your company obtain and verify this consent?	<p>Where there are no systems in place to obtain parental consent, children under the age of consent for data processing may be excluded from using services that would otherwise benefit them. U.S. law sets out various ways in which parental consent can be sought,¹⁷ while European law requires that companies make reasonable efforts to verify parental consent.¹⁸</p>
<input type="checkbox"/> In what circumstances, if any, does your company seek to verify the age of its users? If age verification is employed, what personal information does your company process?	<p>Age verification techniques can help to ensure that consent protocols are met, but can also pose risks to children’s and other users’ privacy by requiring the collection of additional personal information. Where age verification is desirable, companies should consider using trusted third party identity authentication providers to minimize the risks attendant to data collection.</p>
<input type="checkbox"/> Does your company limit the amount of personal data required from children to use a website, platform, service, product or application? What data, if any, are children required to provide?	<p>Under the principle of data minimization, data collection on children should be limited to what is necessary for a specific purpose, such as to provide a website, platform, product, service or application.¹⁹ Children should be informed about the purposes for which their data are collected, including when solely for the purposes of advertising.</p>
<input type="checkbox"/> Is the use of your company’s websites, platforms, products, services or applications conditional on the provision of personal data?	<p>Conditioning the use of a website, platform, product, service or application on the provision of personal data may incentivize children to reveal more personal data than is necessary, and may run counter to the voluntary nature of consent. To avoid this, companies could consider making available a version of their website, platform, product, service or application that does not require children to provide personal data.</p>
<input type="checkbox"/> Does your company process sensitive data relating to children, including biometric data? ²⁰	<p>Processing children’s sensitive data merits additional care, protection and scrutiny, and may be best avoided in many circumstances. Under European law, processing “special categories of data” is permitted only with explicit informed consent, where the data subject makes the information public or in other limited circumstances.²¹ As biometric identification technology involves sensitive personal data, processing children’s biometric information warrants additional protection, such as completing a Privacy Impact Assessment.²²</p>

¹² See European Union General Data Protection Regulation (GDPR), Recital 38.

¹³ GDPR, Recital 32.

¹⁴ GDPR, Article 6.

¹⁵ See United States Children’s Online Privacy Protection Act (COPPA).

¹⁶ GDPR, Article 8(1).

¹⁷ COPPA, §312.5 (b).

¹⁸ GDPR, Article 8(2).

¹⁹ GDPR, Article 6(1)(c).

²⁰ Sensitive data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; biometric data for uniquely identifying a natural person; genetic data; data concerning health; and data concerning sexual activity or orientation.

²¹ GDPR, Article 9.

²² A Privacy Impact Assessment is an internal evaluation of the impact that an envisaged processing operation would have on the protection of personal data (see GDPR, Section 3).

SPECIFIC QUESTIONS FOR CONSIDERATION	CONTEXT
Online platforms and services	
<input type="checkbox"/> Does your company always rely on consent as the legal basis for collecting children’s personal information? If not, on what other legal bases does your company rely? How does your company communicate this to children?	Seeking consent for data collection empowers children and gives them greater control over their personal data. Although collecting children’s personal data may be permitted for other reasons, children should be informed and educated about why and how their data are being collected.
<input type="checkbox"/> Does your company use children’s personal data to develop profiles or for marketing purposes?	Children’s rights may be best protected when their personal data are not used for profiling or targeted marketing, as recognized under European law. ²³ Such protection might include refraining from these practices for younger children, informing children of their right to object to direct marketing, and educating children on how to protect their personal data. ²⁴
<input type="checkbox"/> Does your company put in place higher default privacy settings for child users?	Children’s privacy is better protected when a website, platform, product, service or application does not share their personal data publicly by default. Children are empowered to protect their privacy when they can easily access and adjust their privacy settings from a range of devices.
<input type="checkbox"/> Does your company provide or host games or applications that provide credits or prizes in exchange for personal data?	Games and applications may entice children to provide additional personal data that is not necessary for the delivery of the service or application in question.
<input type="checkbox"/> Does your company provide or host games or applications that turn on a device’s webcam?	Activating a webcam can disclose sensitive personal data, especially where children are displayed on camera. Webcams should not be activated automatically when playing a game or using an application, but rather the explicit and informed consent of the child or their parent or guardian should be sought before a webcam is switched on.
<input type="checkbox"/> Does your company permit third party data collection on your website, platform, product, service or application?	When websites, platforms, products, services or applications facilitate the collection of children’s personal data by other actors, it is important that children or their parents understand and consent to the full scope of data collection involved. In addition, it may be important for companies to ensure that any third parties collecting data through their website, platform, product, service or application respect the company’s practices regarding children.

²³ GDPR, Recital 38. In addition, the European Union’s Article 29 Data Protection Working Party has asserted that companies should, in general, refrain from profiling children for marketing purposes. Article 29 Working Party Guidelines on Automated

Decision-Making and Profiling, available at <<https://www.twobirds.com/en/news/articles/2017/global/article-29-working-party-guidelines-on-automated-decision-making-and-profiling>>.

²⁴ See id.; GDPR, Article 21.

SPECIFIC QUESTIONS FOR CONSIDERATION	CONTEXT
Telecommunications and Internet service providers	
<input type="checkbox"/> How does your company know when a user is a child?	Although communications service providers may not directly engage with children as customers, many users of these services are children. Respecting children’s rights may require understanding which users are children to afford them specific protection.
<input type="checkbox"/> What steps does your company take to protect the personal data of children who use your services?	When children’s personal data are processed, whether children are customers or users, they should be informed of how their personal data are being used and for what purposes. Similarly, adult customers should be educated and empowered to protect the personal data of child users.
Devices and toys	
<input type="checkbox"/> Are your company’s products designed with children’s privacy in mind?	Privacy by design involves bringing data protection considerations into the development of a product, as recognized and required under European law. ²⁵ For example, the design process might seek to minimize how much personal data from children a device collects or transmits.

²⁵ GDPR, Article 25.24 See id.; GDPR, Article 21.

2 USING AND RETAINING CHILDREN'S PERSONAL DATA

Personal data collected from children should be treated in a fair, lawful manner and processed in accordance with well-established data protection principles. Collecting children's personal data should be limited to what is necessary for the use and delivery of websites, platforms, products, services or applications, and children's personal data should not be used for purposes outside their consent or knowledge. In this context, the processing of children's personal data for the purposes of marketing raises concerns as it can be especially difficult for children to understand how their data are processed and shared for monetization. For this reason, companies bear an even greater responsibility to assist children in understanding and exercising their data protection rights. Limiting the collection, processing and retention of children's personal data can also help to prevent loss, theft and misuse, and these data should be accorded the highest organizational and technical protection. It is important that any personal data collected from or about children be accurate and up to date, and children should have the right to correct or request the deletion of their data.

GENERAL QUESTIONS FOR CONSIDERATION	CONTEXT
<input type="checkbox"/> Does your company explain to children, or their parents or guardians, how and why children's personal data will be processed?	It is vital that children, or their parents or guardians, understand how and why their personal data will be processed, including when this data will be used in profiling or for marketing purposes. This allows for fully informed decisions about managing children's privacy online.
<input type="checkbox"/> Does your company give children the opportunity to make meaningful choices about how their personal data are used?	Privacy may be protected through offering choices about how personal data are processed, empowering children, or their parents or guardians, to make clear decisions about the purposes for which their data can be used. These choices are facilitated where there is easy access to information about how children's data are used, and where fresh consent is sought for any proposed changes to the terms and conditions for data processing that may have an impact on a child's personal data or use of the website, platform, product, service or application.
<input type="checkbox"/> Does your company sell or share children's personal data, including data on phone, Internet or device use, to third parties?	Seeking children's, or their parents' or guardians', consent for any onward sale or disclosure of personal data gives children greater control over who can access their personal data.

²⁶ GDPR, Recital 38.

²⁷ GDPR, Article 21. In addition, the European Union's Article 29 Data Protection Working Party has asserted that companies should, in general, refrain from profiling children

for marketing purposes. Article 29 Working Party Guidelines on Automated Decision-Making and Profiling, available at <<https://www.twobirds.com/en/news/articles/2017/global/article-29-working-party-guidelines-on-automated-decision-making-and-profiling>>.

GENERAL QUESTIONS FOR CONSIDERATION	CONTEXT
<input type="checkbox"/> Does your company target behavioural advertising to children?	Behavioural advertising involves collecting and aggregating personal data, which can put children’s privacy at risk. European law suggests that companies should apply specific protection with respect to using children’s personal data for profiling or marketing purposes. ²⁶ Such protection might include refraining from these practices for younger children, informing children of their right to object to direct marketing, and educating children on how to protect their personal data. ²⁷
<input type="checkbox"/> Does your company store children’s personal data securely?	Appropriate technical and organizational data security measures should be in place to prevent breach, fraud and misuse, including a system to notify children, or their parents or guardians, when their data have been unlawfully obtained or intercepted.
<input type="checkbox"/> What processes does your company have in place to ensure that only authorized staff have access to children’s personal data?	Children’s personal data must be sufficiently protected from theft, loss and misuse, including through authorized channels. Organizational protocols such as password protection can provide additional levels of internal security, and access to children’s personal data is best limited to those with a direct role in its processing.
<input type="checkbox"/> Does your company disclose children’s personal data to public authorities in a manner that safeguards their privacy?	Requests for children’s personal data from law enforcement and other public authorities are best handled under a transparent policy framework to ensure any disclosures are consistent with children’s right to privacy. These requests need only be honoured where a legal obligation exists, such as an order from a court or other independent authority, or where the disclosure is in the vital interests of the data subject, for example in circumstances where a child’s life is at risk. The number and type of requests for children’s personal data can be publicly reported to facilitate greater transparency.
<input type="checkbox"/> Does your company provide children, or their parents or guardians, a means to correct or request the deletion of their personal data?	The ability to access, correct and erase personal data is especially important for children, as data gathered during childhood might be processed later to determine access to services in adulthood.
<input type="checkbox"/> Does your company delete or anonymize children’s personal data when it is no longer necessary for the use or provision of your company’s websites, platforms, products, services or applications?	Children’s personal data need not be retained for longer than required for the use and delivery of a website, platform, product, service or application. Along these lines, European law requires that data be held in a de-identified form once they are no longer necessary for the purposes for which they were collected. ²⁸

²⁸ GDPR, Article 6(1).

SPECIFIC QUESTIONS FOR CONSIDERATION	CONTEXT
Online platforms and services	
<input type="checkbox"/> Does your company provide children an easily accessible way to request the deletion of their images or content related to them?	Children can be empowered to request that their personal data be deleted, as required in some circumstances under European law. ²⁹ Simplified and expeditious mechanisms to flag and request that photos and other information be deleted can help children to seek the removal of their personal data.
<input type="checkbox"/> Does your company provide children with an option to close their accounts? If so, does your company delete all personal data held in relation to children's accounts upon closure?	Children are best empowered to protect their privacy when given the option to request the full deletion of their personal data should they no longer wish to use a website, platform, product, service or application.
Devices and toys	
<input type="checkbox"/> Does your company clearly set out the full range of children's personal data that will be collected and transmitted in a form and manner accessible to children and their parents or guardians?	Children and their parents or guardians should be able to easily see and understand how devices and toys collect information, the nature and extent of the information collected, and how this information will be used. To address potential privacy concerns, companies could provide an option to use the core functions of a connected device that does not require sharing certain personal data.
<input type="checkbox"/> Does your company have technical security measures in place for the transmission of children's personal data?	All devices that transmit children's personal data should be equipped with state-of-the-art hardware and software security measures to ensure sufficient protection.
<input type="checkbox"/> Does your company automatically install or push security updates to devices?	Securing children's personal data requires that up-to-date security software be installed and maintained on all transmitting devices.

²⁹ GDPR, Article 17(1)(f).

3 ENSURING CHILDREN'S ACCESS TO INFORMATION

While children have the right to be protected from online violence and discrimination, these rights must be balanced with consideration of their rights to freedom of expression and access to information in the digital world, particularly through online platforms and services. For instance, filtering and removing illegal or harmful content can help to protect children online, but should not infringe on children's rights to share their views or access beneficial information. Similarly, blocking and monitoring tools can help empower parents or guardians to guide children in safely exploring the Internet, but should bear in mind children's growing autonomy to exercise their expression and information rights. Generally, efforts should be made to provide beneficial information and content online in a manner that is accessible to children with regard to their evolving capacities.

GENERAL QUESTIONS FOR CONSIDERATION	CONTEXT
<input type="checkbox"/> Does your company make terms and conditions accessible for children?	<p>For children to understand the terms and conditions for the use of a website, platform, product, service or application, these must be sufficiently clear, concise, accessible and adapted to their level of understanding. European law prescribes that companies must provide individuals with information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child".³⁰ Creative means can be used to communicate the content of terms and conditions to children, such as diagrams, images and videos.</p>
<input type="checkbox"/> Do your company's terms and conditions explicitly state how websites, platforms, products, services or applications can be used? If so, what content or activity does your company consider unacceptable?	<p>Setting out straightforward policies that govern acceptable conduct can encourage responsible behaviour and help children feel more secure and confident in expressing themselves online, while avoiding the risk of arbitrary content removal.</p>

³⁰ GDPR, Article 12(1).

SPECIFIC QUESTIONS FOR CONSIDERATION	CONTEXT
Online platforms and services	
<input type="checkbox"/> Can children easily report inappropriate, illegal or harmful content, or other violations of your company's terms and conditions?	<p>Simple, easily accessible mechanisms to flag or report potentially problematic content can help empower children to safely exercise their expression and information rights online.</p>
<input type="checkbox"/> Does your company have a process in place for children to contest the removal of their content?	<p>Content removal can be made more accurate and accountable through rigorous and transparent processes that allow for the review of contested decisions.</p>
<input type="checkbox"/> Does your company permit children to use pseudonyms online?	<p>Permitting the use of pseudonyms provides children the option to remain anonymous online, which may be particularly important for children at risk of becoming vulnerable or marginalized.</p>
<input type="checkbox"/> Does your company filter content displayed to children because of their age?	<p>It is important to be open and transparent about measures that filter the content children can view or access. To make informed choices, children, and their parents or guardians, will need a clear understanding of what content is being or could be filtered.</p>
Telecommunications and Internet service providers	
<input type="checkbox"/> Does your company block websites or content above and beyond what is required by law?	<p>Blocking and filtering content that is not illegal may threaten children's access to otherwise beneficial information. To make informed choices, children, and their parents or guardians, will need a clear understanding of what content is being or could be filtered.</p>
<input type="checkbox"/> Does your company provide parental control filters, either on an 'opt-in' or an 'opt-out' basis? If so, are these mechanisms secure, adjustable and transparent?	<p>Parental controls can empower parents to help their children safely exercise their rights online, and offering parental control filters on an 'opt-in' basis helps to ensure that parents or guardians have made an active and informed choice to filter the content that their children can access. Parental control filters should not collect any more data than is necessary for their delivery, and should provide high levels of security for children's data. Filters can more effectively and appropriately protect children when they are adjustable to suit a child's evolving capacities, and should provide transparency to both parents or guardians and children about the nature of the content being blocked.</p>
<input type="checkbox"/> Does your company give users the option to report suspected instances of over-blocking?	<p>Children, and their parents or guardians, should be able to raise concerns where otherwise beneficial content has been blocked or filtered.</p>

SPECIFIC QUESTIONS FOR CONSIDERATION	CONTEXT
Devices and toys	
<input type="checkbox"/> Does your company incorporate parental control mechanisms in its products, on either an 'opt-in' or an 'opt-out' basis? If so, are these mechanisms secure, adjustable and transparent?	<p>Parental controls can empower parents to help their children safely exercise their rights online, and offering parental control mechanisms on an 'opt-in' basis helps to ensure that parents or guardians have made an active and informed choice to filter the content that their children can access. Parental control mechanisms should not collect any more data than is necessary for their delivery, and should provide high levels of security for children's data. Filters can more effectively and appropriately protect children when they are adjustable to suit a child's evolving capacities, and should provide transparency to both parents or guardians and children about the nature of the content being blocked.</p>

4 EDUCATING AND INFORMING CHILDREN ONLINE

Navigating the online environment can be especially challenging for children, who often do not understand the commercial nature of the Internet. As it is increasingly difficult for children to grasp how their personal data are being collected, processed, shared and monetized online, it is ever more critical that children are educated and informed about how to manage their privacy. Similarly, given children’s developing levels of digital literacy, it is important that online commercial content be adequately identified as such. Children should be equipped with the information and skills necessary to enjoy their privacy, protect their reputation and exercise their freedom of expression online.

GENERAL QUESTIONS FOR CONSIDERATION	CONTEXT
<input type="checkbox"/> Does your company provide resources for children and their families about protecting children’s privacy online?	Whenever a website, platform, product, service or application collects children’s personal data, there is an opportunity to engage children in ways that help them to manage their privacy online. Along these lines, resources may be made available to children and their families to support the development of children’s digital literacy, including information about privacy and expression rights in the digital environment.
<input type="checkbox"/> Does your company educate and encourage children to behave responsibly online?	Terms and conditions can define and encourage responsible behaviour online, and content moderation policies and decisions provide an avenue to engage children in an ongoing discussion. To be accessible for children, terms and conditions should be concise, presented in plain language and go beyond written communication. Additional tools and resources can also help children understand how to behave responsibly online, to report and refrain from cyberbullying and other forms of abuse, and to protect their personal data and reputation.
<input type="checkbox"/> Does your company have policies in place and take measures to ensure that advertising is effectively identified as commercial content?	Depending on their age and maturity, children may struggle to identify the commercial nature of promotional content. As new techniques such as advergames, native content and the use of influencers can make it increasingly difficult for children to identify commercial messages, it is important that all commercial content be clearly identified as such in a way that children can easily see and understand.

SPECIFIC QUESTIONS FOR CONSIDERATION	CONTEXT
Online platforms and services	
<input type="checkbox"/> Does your company provide a range of privacy settings for children’s online profiles?	Children can be empowered to express and protect themselves online by having full control over their online profiles, including who can access information, who can post content, and what content is shared.
<input type="checkbox"/> Does your company provide default settings for children’s profiles that protect their online privacy?	Children can learn to safely exercise their right to freedom of expression in online environments where their privacy is protected, including through default profile settings that limit information sharing beyond personal contacts.
<input type="checkbox"/> Are children easily able to change the privacy settings for their online profiles?	Children are able to express and protect themselves online more fully when they can easily access and adjust their privacy settings from a range of devices. Where children seek to change privacy settings in a way that would make information on their profiles publicly available, additional prompts could help children to understand the implications of sharing information publicly and reconfirm their intention to do so.

