LAW LIBRARY
LIBRARY OF CONGRESS

Ireland: Data Protection and Children

June 2021

LL File No. 2021-020231
LRA-D-PUB-002464

The Law Library of Congress, Global Legal Research Directorate
(202) 707-5080 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

Contents

Ireland: Data Protection and Children

Clare Feikert-Ahalt
Senior Foreign Law Specialist

SUMMARY Ireland implemented the Data Protection Act in 2018 to give effect to certain aspects of the General Data Protection Regulation (GDPR) and establish the Data Protection Commission (DPC). This framework regulates how personal data may be processed. The processing of children's personal data is afforded special protection under both the act and the regulation. In addition, the DPC published a draft code, *Fundamentals for a Child-Oriented Approach to Data Processing* (known as "the Fundamentals"), as required under the Data Protection Act, for public consultation in December 2020. The commissioner is currently considering feedback from the public. The draft Fundamentals cover measures that organizations must take before processing the data of children and highlight that the best interests of the child takes precedence over any legitimate business interests. The DPC has stated that, once the draft Fundamentals are finalized, an organization's compliance with the Fundamentals will be taken into consideration when assessing whether it has met the obligations of the GDPR.

Advertising in Ireland is self-regulated by a series of voluntary industry codes, as well as through legislation and the EU's Audiovisual Media Services Directive. Profiling, behavioral advertising, and automated decision-making in relation to children or the use of a child's personal data for marketing or advertising will be restricted under the draft Fundamentals.

I. Introduction

The European Union's (EU) General Data Protection Regulation (GDPR)[1] has direct effect, meaning it requires no implementing legislation to bring its provisions into force in Ireland. The GDPR contains certain aspects that provide member states with flexibility over how to implement it, such as such determining the digital age of consent, and, as "a principles-based law, the rules are set out in it in very broad terms. The GDPR does not generally address how those rules should be interpreted and applied in specific situations."[2] As a result, Ireland has enacted the Data Protection Act 2018 (the DPA), which entered into force on May 25, 2018, "to give further effect to certain aspects of the rules in the GDPR."[3] The DPA established the Data Protection Commission (DPC) to enforce the legislation and established the age of digital consent for children in Ireland as 16 years.

The DPA and GDPR regulate how personal data may be processed. These laws provide for general principles of data protection, which place a duty on data controllers to

[1] General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1, https://perma.cc/7T85-89ZQ.

[2] Data Protection Act 2018, No 7 of 2018, https://perma.cc/N5RF-CXDG.

[3] Id.

- obtain and process data lawfully and fairly,
- only collect data for specific legitimate purposes and not process it in a way that is incompatible with that purpose,
- ensure that any data collected is accurate, relevant, and not excessive for the reason it is processed,
- process data in a way that ensures its security, and
- keep data in a way that enables the identification of the "subject for no longer than is necessary for the purposes for which the data are processed."[4]

Article 6 of the GDPR provides six legal bases under which data may be obtained and processed lawfully and fairly. The most common of these legal bases is when data subjects consent to the processing of their data for one or more specific purposes. The other legal bases are when data processing is necessary to

- perform, or enter into, a contract,
- comply with a legal obligation,
- protect the vital interests of the data subject or another person,
- perform a task in the public interest or through official authority, or
- where the legitimate interests of the data controller are not outweighed by either the data subjects' interests or fundamental rights and freedoms.[5]

The law further provides data subjects with certain rights, such as the right to access data, have data erased, restrict processing, and object to their data being processed.[6]

One in three internet users in Ireland is a child.[7] Ireland published, in draft form, the *Fundamentals for a Child-Oriented Approach to Data Processing* (the Fundamentals) for public consultation in December 2020, as required under the DPA. The draft Fundamentals are 14 matters that aim to

> introduce child-specific data protection interpretative principles and recommended measures that will enhance the level of protection afforded to children against the data processing risks posed to them by their use of/access to services in both an online and offline world. In tandem, the Fundamentals will assist organisations that process children's data, by clarifying the principles, arising from the high-level obligations under the GDPR, to which the DPC expects such organisations to adhere.[8]

[4] Id. § 71.

[5] GDPR, art. 6.

[6] Data Protection Act 2018, §§ 89-95.

[7] Data Protection Commission (DPC), *Foreword* to *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing* (Dec. 2020), https://perma.cc/NFA6-2A77.

[8] Id.

The draft Fundamentals apply to data collected about children both on and offline. The DPC notes that its draft Fundamentals differ from the United Kingdom's (UK's) *Age Appropriate Design Code*, being broader and "not focused solely on the engineering and design of online products and services."[9] While noting this difference, the DPC has stated that the Fundamentals "are entirely consistent with the UK Code and in particular it is clear that the best interests of the child principle underpin both."[10]

II. Data Protection for Children

The DPA defines children as those under 18 years of age, with the exception that the age of digital consent for a child in relation to information society services is 16 years old.[11] The DPA obligates the DPC to issue a code of conduct to assist people in accurately applying the GDPR, notably with regard to how to protect children, how consent from a child's parent or guardian should be obtained, how safeguards should be integrated into data processing to protect children's rights in an age-appropriate manner, and how the personal data of children is processed for direct marketing and user profiles.[12] In making the code, the DPA is clear, in accordance with the United Nations Convention on the Rights of the Child (UNCRC), that the best interests of the child should be paramount and that the child's rights should be protected.[13]

As noted above, the DPC published a consultation paper seeking comments on the draft Fundamentals in December 2020. The consultation period closed at the end of March 2021.[14] The draft Fundamentals note:

> While there are a small number of provisions in the 2018 Act which concern processing of children's personal data, for the most part these do not elaborate on how the general rules in the GDPR should be applied where children are concerned.
>
> It is important to highlight that these Fundamentals focus on child-specific provisions and so should not be taken to be the sum total of all obligations that apply under the GDPR.[15]

The draft Fundamentals consist of 14 matters that establish "the baseline expectations of the DPC as the regulator in Ireland for the processing of children's personal data."[16] They are designed to clarify the principles contained in the GDPR as they apply to children in order to help data controllers understand the measures required to protect children from the risks posed by data processing when they access services.[17]

---

[9] Id.

[10] Id.

[11] Data Protection Act 2018, §§ 29, 31.

[12] Data Protection Act 2018, § 32.

[13] DPC, supra note 7, at 19.

[14] Id.

[15] Id. at 12.

[16] Id. at 14.

[17] Id. at 16.

A. Who Should Comply with the Fundamentals

Once the draft Fundamentals are finalized, organizations that provide a service directed at, intended for, or which is more likely than not to be accessed by children, should comply with the Fundamentals.[18] Examples given by the DPC as services likely to be accessed by children include educational providers, sports and social clubs who collect such information offline, and online providers, such as websites, apps, and services such as social media, entertainment, health and social care and support services.[19] There are a number of factors that a site can use to determine the age of its users, for example, considering the content provided on the site.[20] The principle of accountability under the GDPR further requires organizations to take steps to determine whether they are collecting personal data from children and, if they determine they are, to take steps to "ensure that they comply with the higher standards of protection required of controllers under the GDPR with regard to the processing of children's data."[21]

B. The Fundamentals

1. "Floor of Protection"

Draft Fundamental 1 requires online service providers to either provide a "floor of protection" by applying the "high standardized level of data protection"[22] required by the draft Fundamentals to all users, or to adopt a risk-based approach, whereby the age of each user must be verified and the draft Fundamentals applied to child users only.[23] While the DPC acknowledges that there is no single standard, or set of standards, that can achieve this draft fundamental, it notes that organizations should consider which are appropriate in the context of its users. The DPC provides several examples, such as high levels of default privacy settings, minimizing the data collected from children, refraining from systematically sharing children's personal data with third parties without clear parental consent, turning off geolocation by default (unless it is necessary for the service being provided), turning profiling off, and avoiding nudge techniques to encourage children to provide unnecessary information.[24] This approach is similar to that adopted by the UK in its Age Appropriate Design Code.

2. "Clear-Cut Consent"

As noted above, one legal basis to process data is provided if the data subject provides their consent, and the age of digital consent is 16 years old in Ireland. Online information society services, excluding preventative or counseling services, must make "reasonable efforts"[25] using

[18] Id. at 15.

[19] Id. at 15.

[20] Id. at 15.

[21] Id. at 15. See also GDPR, art. 24.

[22] Id. at 16.

[23] Id. at 15.

[24] Id. at 59.

[25] Id. at 40.

available technology to verify both the age of the user and, if required, that the consent of a person with parental authority for children under this age has been given in order to process the child's personal data.[26]

There are no specific requirements as to the methods organizations should use, other than that they should be appropriate, proportionate, and use the technology available to them. The DPC notes that "organisations must fully explore all of the technological options available to them—and maximise innovation,"[27] but that any methods used should not be overly intrusive and should comply with the data protection principles. The DPC gives examples used in the United States by the Federal Trade Commission, such as requiring the use of a credit card, or providing government identification, to ensure consent is correctly obtained, but notes that it is the responsibility of the organization to determine the most appropriate verification method.[28]

Any consent given must be "freely given, specific, informed and unambiguous made by way of a clear statement or affirmative action by the data subject. The consent must also be distinguishable from other matters and possible to withdraw at any time."[29]

The DPC notes that any requirements surrounding the age of digital consent must not impose restrictions on a child's ability to access a service and also highlights there are five other bases, referred to above, which provide a lawful reason for processing personal data.[30] If a parent provides their consent, the organization must continue to comply with the draft Fundamentals regarding any data generated by the child user.

3. "Zero Interference"

Online service providers may process children's personal data under one of the lawful bases provided by article 6 of the GDPR described above; however, the draft Fundamentals indicate the DPC will take a very narrow approach regarding when the processing of such data will be lawful. Moreover, if an organization determines that a lawful basis to process personal data is in its legitimate interests, it must take a case-by-case approach to ensure that any processing of children's data does not "interfere with, conflict with or negatively impact, at any level, the best interests of the child,"[31] known as the principle of zero interference with the best interests of a child.

4. "Know Your Audience"

The DPC notes that guidance from the European Data Protection Board on transparency provides that organizations should know their users, or the people about whom they collect information.

[26] Data Protection Act 2018 § 31;GDPR, art. 8.

[27] DPC, supra note 7, at 40.

[28] Id.

[29] Id. at 22.

[30] Id. at 39.

[31] Id. at 24.

Knowledge of users can be gathered using artificial intelligence, or by user testing and market research. The DPC further states that a risk-based approach should be adopted to verify the age of the child, with the measures required varying according to the type and sensitivity of data being processed, whether the personal data is accessible to others, and the kind of service being offered.

The DPC states that, where a service provider believes it cannot prevent children under the age of consent from accessing its services, it must implement higher standards for data protection measures for all users to safeguard child users. The DPC further notes that the most stringent age verification methods are necessary for age-restricted services, such as pornography or gambling.[32]

5. "Information in Every Instance"

Children must receive information about how their personal data is processed and used under each lawful basis, even where a legal guardian has given consent to processing the data.[33] This information should be provided in clear and concise language that is appropriate for the child's age, capacity, and development, and this overlaps, in part, with draft Fundamental 6, discussed below.

6. "Child-Oriented Transparency"

Article 12 of the GDPR requires organizations to provide information—known as transparency information—about how personal data is used. It should be "provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language,"[34] or through cartoons, videos, or other non-textual methods that are clear and understandable to children. Given the different developmental stages of children, draft Fundamental 4 overlaps with this, as organizations must know who their audience is so that information can be tailored to ensure that it is understandable for the different ages and stages of child users.[35] The DPC notes that this does not mean that there must be multiple sets of transparency information in cases where an organization has mixed users, as information that is easily understood by a child will comply with the transparency requirements for adult data subjects.[36]

Transparency information should be provided to students, not just during the initial point of collecting data, but also at other points. Organizations are encouraged to use just-in-time notifications, such as before they share or post information.

[32] Id. at 44.

[33] Id. at 26.

[34] Id.

[35] Id.

[36] Id.

7. "Let Children Have Their Say"

This draft Fundamental addresses how children may exercise their rights over their personal data. Ireland does not have a law that specifies an age at which children can legally exercise their rights as a data subject. The DPC undertook research to determine whether it should set an age at which this can occur, but concluded that it was not "appropriate to set a general age threshold as the point at which children should be able to exercise their rights on their own behalf . . . as age alone is not the most appropriate benchmark."[37] Instead of using age, the DPC set a number of factors that organizations must consider when determining whether children have the capacity, and whether it is in their best interests, to exercise their rights as data subjects, including:

- The age and maturity (for example as demonstrated by interactions between the child and the organisation in question) of the child;
- The type of request (access request, erasure request, right to object, etc.);
- The context for the processing and the type of service offered by the controller (e.g. social media platform, doctor-patient relationship, online shopping platform, etc.);
- The type of personal data at issue (e.g. child seeking access to medical data, child seeking erasure of photos of themself on social media, child seeking to update their email address on a platform) . . .
- Whether enabling the child to exercise their data protection rights themself is in the best interest of the child (i.e. do they understand the consequences of erasing certain types of personal data, will they fully comprehend what it is they are receiving as part of an access request, will receiving certain information be detrimental to their well-being?)
- Whether the child is seeking to exercise their rights with the assistance/ participation/ knowledge of a parent/ guardian or expert third party/ advocate.[38]

While the DPC has listed these criteria, it has stated that children should be able to exercise their rights as a data subject "and should not be prevented from doing so as a result of their age, maturity or capacity."[39] In some instances, parents or legal guardians may act on the child's behalf to exercise the child's rights as a data subject. In these instances, there is a rebuttable presumption that the parent or legal guardian is acting in the best interests of the child.[40]

8. "Consent Doesn't Change Childhood"

Where consent is obtained from the child or guardian, this draft Fundamental requires that such consent does not result in children being treated in the same manner as adults. It also highlights that digital consent should not be used to prevent children from accessing a service. Overlapping with draft Fundamental 2, consent must be freely given, specific, informed, unambiguous, and able to be withdrawn at any time.

[37] Id. at 33.

[38] Id. at 34.

[39] Id. at 35.

[40] Id.

9. "Your Platform, Your Responsibility"

Draft Fundamental 9 highlights the difference between age verification that organizations must undertake to verify whether a user is under the age of 18 and thus requires higher standards of data protection and age verification to check whether a user is under the age of 16 and processing the user's data requires a guardian's consent.[41] In the case of consent, age verification is not required to comply with the law but, as noted above, companies must make reasonable efforts to verify that consent is given on behalf of a child under the age of 16 by the child's legal guardian using available technology.[42]

The DPC notes that companies making money from the provision or sale of services using digital and online technology must be held to a higher standard when verifying the age of a child or obtaining the consent of a guardian for processing this data and must ensure that the measures it uses are effective.[43] As noted above, the DPC considers that organizations should adopt a proportionate, risk-based approach to verify both age and that consent has been given by the guardian of the child user, the method of which should be determined by the organization itself and should be kept under review.[44]

10. "Don't Shut Out Child Users or Downgrade Their Experience"

This draft Fundamental states that organizations should not restrict children from using its services, or provide children with a lesser experience, to comply with data protection laws:

> The DPC considers that the user experience offered to child users should be adapted in order to minimise, to the greatest extent possible, the risks posed to children from the processing of their personal data in the context of using/ accessing a service, without a deterioration in the overall user experience and the availability of the central features, for which children primarily access the service.[45]

Failing to do this can have implications for the rights of children, provided for in the United Nations Convention on the Rights of the Child, notably the right of the child to express their views, to seek, review and import information and ideas and their right to freedom of expression.[46] Creating a separate experience for child users also poses a risk of leading children to lie about their age, which can result in lesser data protection standards being applied to them.

11. "Minimum User Ages Aren't an Excuse"

This draft Fundamental clarifies that organizations cannot avoid the requirements of the GDPR, DPA, and the draft Fundamentals by requiring a minimum age for users. Organizations that opt

[41] Id. at 39.

[42] Id.

[43] Id.

[44] Id. at 41.

[45] Id. at 42.

[46] Id.

to have a minimum age have an obligation to ensure that age verification measures used are effective and, if children are able to circumvent these measures, the organization must ensure that high levels of data protection are in place to safeguard child users, even if these users are below the minimum age required by the organization.[47]

12. "Prohibition on Profiling"

Draft Fundamental 12 provides that organizations should not profile children, use automated decision-making in relation to children, or use a child's personal data for marketing or advertising purposes unless it is clearly in the best interests of the child to do so.[48] This is due to the child's "vulnerability and susceptibility to behavioral advertising. This is especially the case for online games and other information society services that use profiling to identify users that can be encouraged to spend more money."[49] The DPC has stated that the circumstances in which these activities will be lawful will be very limited and that any organization that determines it has the legal basis to profile, or engage automated decision-making about, children must conduct a Data Protection Impact Analysis (DPIA) and have safeguards in place to protect children.[50]

Direct marketing is governed by the ePrivacy Regulations, which require organizations to have the consent of individuals before they can directly send messages to them. In order to send electronic direct marketing communications to a child, the organization must have consent, which may be withdrawn. The DPC notes that "it is likely the age of digital consent . . . applies to electronic direct marketing communications which are sent by SMS and email as it would seem that communications sent by these modes fall within the definition of 'information society services'," [51] and thus, the consent of a legal guardian must be obtained for children under the age of 16. For other types of direct marketing, there is no minimum age requirement to obtain the consent of a child under the age of 16. The DPC states: "In theory this means that organisations can conduct some marketing activities towards children where their consent has been obtained. However in any case where an organisation is considering directing marketing activities towards children, it should be extremely cautious about doing so."[52]

The organization must obtain consent from the child or guardian, which must be freely given, specific, and unambiguous, and the child or guardian must be fully informed about how the personal data will be used.[53] In all instances, the best interests of the child must be the foremost consideration, and the organization must be able to demonstrate that its activities align

> with the DPC's position that there should be zero interference with the best interests of the child in the processing of their personal data. Therefore unless an organisation can show

[47] Id. at 43.

[48] Id. at 54.

[49] Id. at 47.

[50] Id. at 54.

[51] Id. at 47.

[52] Id. at 49.

[53] Id.

> that the direct marketing activities in question which rely on the processing of children's personal data to carry out the marketing positively promote the best interests of the child (irrespective of the legal basis being relied on to do so), such activities should not be undertaken. Examples of areas where direct marketing may be used to positively promote the best interests of children include direct marketing of: counselling or support services; educational, health and social services; and advocacy and representative organisations.[54]

Behavioral advertising, based upon user profiles is frequently facilitated by the use of cookies and is regulated, in part, by the ePrivacy Regulations. As noted above, these Regulations require that, other than for cookies that are strictly necessary, consent must be obtained from the user, which must be provided in clear and easily understandable terms. The processing of any personal data that is created from the use of cookies must comply with the requirements of the GDPR.

13. "Do a Data Protection Impact Analysis"

The DPC has stated that DPIA will be mandatory for organizations whose services are intended for, directed at, or likely to be accessed by children.[55] DPIAs must identify risks that may arise from the processing of personal data and how these risks will be minimized. The DPC has stated

> [s]uch risk assessments should take account of varying ages, capacities and developmental needs of child users as well as considering both actual and potential risks arising from data processing to the health, well-being and general best interests of the child, including social, mental, physical and financial harm.[56]

The aim of DPIAs is to minimize the risks posed to children that arise from the processing of their personal data. The DPC has stated that a DPIA, or lack thereof, will be a factor that it considers when assessing whether the organization complies with its obligations under the GDPR and that "a child-oriented DPIA is the first step in mitigating risk arising from processing children's personal data, and will be seen as a key act of compliance with existing legal requirements for protecting the position of children as data subjects."[57]

Thus, a well-considered DPIA is an essential step for organizations to take in order to help mitigate any liability under the DPA.

14. "Bake It In"

This draft Fundamental requires online service providers to have a high level of data protection by design and default that is consistent across its services:

> [D]ata protection measures should be built into the architecture and functioning of a product or service from the very start of the design process (rather than being considered

[54] Id. at 51.

[55] Id. at 57.

[56] Id. at 58.

[57] Id. at 58.

> after the development phase) and that the strictest privacy settings should automatically apply to a product or service.[58]

The DPC notes that there is no single standard that can apply to all organizations, but that an organization should be able to show how its measures represent best practice in data protection and how the best interests of the child are reflected across the design, development, implementation and operation of services that are directed at, intended for, or likely to be accessed by children as well as how effective the measures are in achieving their aim. The DPC has further stated "[t]he principle of the best interests of the child must be a key criterion in any DPIA and must prevail over the commercial interests of an organization in the event of a conflict between the two sets of interests."[59] It further notes that if a high level of data protection is in place by design and default, this will help ensure that children are not targeted with advertisements for age-restricted content.[60]

C. Penalties

The DPA contains a series of offenses, such as the unauthorized disclosure of personal data by a processor or the disclosure of personal data obtained without lawful authority, both of which are punishable by a fine of up to €50,000 (approximately US$61,000) and/or five years of imprisonment. The DPC also has the power to issue administrative fines of up to €10 million (approximately US$12 million) or up to 2% of the worldwide annual turnover of an undertaking for infringements of the GDPR.[61]

Ireland has a large number of technology companies with headquarters in its jurisdiction and it has been criticized by the European Parliament for failing to sanction companies that are found to be in breach of the GDPR and DPA, with the DPC closing most cases using a settlement. In March 2021, the European Parliament called upon Ireland to

> speed up their ongoing investigations into major cases in order to show EU citizens that data protection is an enforceable right in the EU; points out that the success of the 'one-stop shop-mechanism' is contingent on the time and effort that DPAs can dedicate to the handling of and cooperation on individual cross-border cases in the EDPB, and that the lack of political will and resources has immediate consequences on the extent to which this mechanism can function properly.[62]

---

[58] Id. at 58.

[59] Id. at 59.

[60] Id. at 42.

[61] Data Protection Act 2018 § 141;GDPR, art. 83.

[62] European Parliament Resolution on the Commission Evaluation Report on the Implementation of the General Data Protection Regulation Two Years After Its Application, 2020/2717(RSP) (Mar. 17, 2021), ¶ 20, https://perma.cc/GY35-QC5M.

III. Advertisements on Platforms Designed for Children

Advertising in Ireland is self-regulated by a series of voluntary industry codes, as well as through legislation and the EU's Audiovisual Media Services Directive (AVMSD). Section 30 of the DPA specifically governs micro-targeting and profiling of children and provides as follows:

> It shall be an offence under this Act for any company or corporate body to process the personal data of a child as defined by section 29 for the purposes of direct marketing, profiling or micro-targeting. Such an offence shall be punishable by an administrative fine under section 141.[63]

This section has not yet been brought into force.

The AVMSD, which is reflected in Ireland's Code of Standards for Advertising and Marketing Communications, aims to protect children, and has been extended to cover video-sharing platforms and audiovisual content shown on social media sites. Video-sharing platforms are under an obligation to take measures, such as age-verification or parental control systems, to protect minors from advertisements that may impair their physical, mental, or moral development. The Code of Standards prohibits advertisements from directing minors to purchase goods or services; from encouraging minors to persuade their parents to purchase goods or services; from including elements that endanger a minor's physical or moral integrity or health and safety; or from exploiting the special trust that minors have in their parents, guardians or teachers.[64] Marketing communications for food, other than for fruit or vegetables, should not be targeted to children under the age of 16 to encourage them to eat or drink a product to take advantage of a promotional offer or create a sense of urgency that encourages the purchase of a large quantity of the product or excessive consumption.[65]

As noted above, profiling, behavioral advertising, and automated decision-making in relation to children or use a child's personal data for marketing or advertising will be restricted under the draft Fundamentals.

Advertisements for age-restricted products should not be directed at, or appeal to, children. For example, the Code of Standards for Advertising and Marketing Communications notes that advertisers should ensure this does not happen "through the selection of media or the context in which they appear." For example, advertisements for e-cigarettes should not be used on a medium where more than 25% of the audience is under the age of 18.[66] Additionally, advertisers

[63] Data Protection Act 2018, § 30.

[64] ASAI, *Code of Standards for Advertising and Marketing Communications in Ireland* ¶ 7.3-7.6 (7th ed., Mar. 2016), https://perma.cc/BA73-E9T4.

[65] Dep't of Health, *Non-Broadcast Media Advertising and Marketing of Food and Non-Alcoholic Beverages, Including Sponsorship and Retail Product Placement: Voluntary Codes of Practice* ¶ 5.2.2 (Dec. 2017), https://perma.cc/TDT2-YAUZ.

[66] ASAI, supra note 64, ¶ 17.10.

should not use media that is primarily targeted at children to promote products that are unsuitable to them.[67]

IV. Future Plans to Protect Children Online

The consultation period for the draft Fundamentals closed on March 31, 2021, and the government is working to finalize the Fundamentals while taking public opinion into account.

[67] Id. ¶ 6.12.