



Universiteit
Leiden
The Netherlands

Child rights impact assessment: impact and legal analysis for the development of the CRIA

Hof, S. van der; Challis, L.; Wanroij, E. van; Schermer, B.W.

Citation

Hof, S. van der, Challis, L., Wanroij, E. van, & Schermer, B. W. (2024). *Child rights impact assessment: impact and legal analysis for the development of the CRIA*. The Hague: Ministry for Internal Affairs and Kingdom Relations. Retrieved from <https://hdl.handle.net/1887/4209969>

Version: Publisher's Version

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/4209969>

Note: To cite this publication please use the final published version (if applicable).



Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

IMPACT AND LEGAL ANALYSIS FOR THE DEVELOPMENT OF THE CRIA

March 2024

*Developed by Leiden University and Considerati,
Commissioned by Ministry of the Interior and Kingdom Relations*

Disclaimer: The translation of the CRIA is solely intended to provide information. The text of the translation is an unofficial translation. The Dutch text of the CRIA is the only authentic and formal text.

Table of contents

GLOSSARY	3
INTRODUCTION	3
1. LAWS AND REGULATIONS AIMED AT PROTECTING CHILDREN	4
1.1. DIGITAL SERVICES FOR 18 YEARS AND OVER	4
1.2. DIGITAL SERVICES ALSO ACCESSIBLE TO PERSONS UNDER 18 YEARS OF AGE	4
1.2.1 PROTECTION OF CHILDREN'S PERSONAL DATA	4
1.2.2 PROTECTING CHILDREN FROM POTENTIALLY HARMFUL CONTENT	8
1.2.2.1 MEDIA ACT	8
1.2.2.2 (OTHER) RIGHT OF CLAIM	10
1.2.3 OTHER CONDITIONS FOR DIGITAL SERVICES ACCESSIBLE TO CHILDREN	13
1.2.3.1 AGREEMENTS ENTERED INTO BY CHILDREN	13
1.2.3.2 BAN ON PROVISION OF ONLINE GAMBLING SERVICES	13
1.2.3.3 CONSUMER LAW	14
1.2.3.4 DIGITAL SERVICES REGULATION (DSR)	16
1.2.3.5 DIGITAL MARKETS REGULATION (DMR)	18
1.2.4 CONDITIONS FOR OFFERING PRODUCTS (ONLINE)	18
1.2.4.1 BAN ON (ONLINE) SALES OF ALCOHOL AND SMOKING PRODUCTS	19
1.2.4.2 BAN ON THE (ONLINE) SALE OF WEAPONS	20
2. RELATIONSHIP OF CRIA TO OTHER RELEVANT GUIDES	20
2.1 THE DUTCH CHILD RIGHTS CODE AND OTHER 'AGE APPROPRIATE DESIGN' INITIATIVES	20
2.2 FRAIA	21
2.3 DPIA CHECKLIST PERSONAL DATA AUTHORITY	21
2.4 UNICEF CHILDREN'S RIGHTS IN IMPACT ASSESSMENT	22
2.5 THE FAIR AND FACT PRINCIPLES	22

Glossary¹

1. **Age estimation:** A system that generally relies on estimation based on inherent characteristics or behaviours of the individual, to determine that the age of the individual is likely to fall within an age range, with a certain degree of reliability, to provide a lower degree of certainty in determining the age or age range of an individual than age verification techniques.
2. **Information society service:** any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services².
3. **Age verification:** A system that generally relies on hard (physical) identifiers and/or verified sources of identification to determine an individual's age or age group.
4. **Lootbox:** a virtual treasure chest/box/crate containing resources (a loot) that the player can use to enhance their gaming experience.
5. **Minor/child:** a natural person under eighteen years of age.
6. **Online platform** means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor or merely ancillary feature of another service or a minor functionality of the main service and cannot, for objective and technical reasons, be used without that other service, and the integration of the feature or functionality into the other service is not a way to circumvent the applicability of this Regulation.³
7. **Online profiling:** any form of automated processing of personal data consisting of using personal data to assess certain personal aspects relating to a natural person, in particular to analyse or predict aspects relating to that natural person's work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
8. **Personal data:** Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be identified, directly or indirectly⁴.

Introduction

The purpose of the impact and legal analysis is to provide background information and frameworks from which to develop the prototype for the CRIA. The structure of the report is as follows: chapter 2 identifies the specific legal safeguards for digital services used by children. Finally, Chapter 3 highlights the relationship of the CRIA to other guidance relevant to protecting children and their rights against online risks from digital services.

- *Are you developing digital services aimed at children? If so, you need to consider the risks they pose to child welfare. In front of you is the Children's Rights Impact Assessment (CRIA). The Ministry of the Interior Affairs and Kingdom Relations commissioned the CRIA to help you identify the potential impact of the digital service on children's rights and welfare.*

1 <https://euconsent.eu/euconsent-common-vocabulary/>.

2 <https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32015L1535&qid=1686150727253>.

3 Article 3(i) DSR.

4 Article 4(1) GDPR.

1. Laws and regulations aimed at protecting children

Children's rights are increasingly protected when using digital services through specific safeguards in current laws and regulations. This chapter provides an overview of specific safeguards in relevant laws. Only legislation applicable to information society services has been included in the analysis.⁵

1.1. Digital services for 18 years and over

Specific legal safeguards for children only need to be taken into account if a digital service is accessible to children (persons under 18). Some digital services are not allowed by law to be offered to persons under 18. Example are online gambling services and services showing audiovisual content classified as 18+. However, providers themselves can decide on other grounds to offer their digital service only to persons aged 18 or older.

- *Is the digital service intended for persons aged 18 and above, and is there no evidence that the digital service is being used by persons under 18?*

If the answer to this question is that the digital service is indeed intended only for persons aged 18 and above, then the specific safeguards do not apply and no CRIA needs to be carried out. However, it is then important that the provider of the digital service can demonstrate that persons under 18 do not use the digital service. This can be done by using a demonstrably adequate form of age verification. 'Demonstrably adequate' means that the method used is provably capable of admitting only users based on the attribute '18 years and older'.

Methods such as 'self-declaration' (users themselves provide their age) and 'age estimation' (age is estimated from biometric characteristics and/or behavioural data) are not demonstrably adequate for this purpose.

1.2. Digital services also accessible to persons under 18 years of age

1.2.1 Protection of children's personal data

The GDPR only applies when personal data are processed (Article 2 (1) GDPR) and the higher level of protection for children (including recital 38 GDPR) is only relevant when personal data of children are processed.

- *Are personal data of persons under 18 being processed?*

If personal data of persons under 18 are processed, the following obligations and concerns for children under the GDPR should be taken into account. It should be assumed that personal data of persons under 18 years of age are processed if no demonstrably adequate age verification has been implemented.

GDPR	
Article 5 GDPR	Principles governing the processing of personal data
Lawful (sub a)	→ Article 6 GDPR
Proper (sub a)	Article 3 UNCRC: is the data processing in the best interests of the child, i.e. does it contribute to the welfare of children, or at least does it not harm
Transparent (sub a)	→ Article 12 GDPR

⁵ Within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535.

Minimum data processing (sub c)	→ Article 25 GDPR
Accountability (paragraph 2)	→ Article 24 GDPR Article 3 UNCRC: obligation to motivate how the best interests of the child have been taken into account in data processing processes

<i>GDPR</i>	
Article 6 GDPR	Lawfulness of processing
Consent (paragraph 1(a))	→ Articles 7 and 8 GDPR
Necessary for the performance of a contract (paragraph 1(b))	Personal data of children can only be processed under this legal basis if children are authorised to enter into a contract under the applicable contract law. A parent may give consent to the child to enter into a contract. This provision contains an implicit obligation to verify the age of the data subject and the consenting person's status as a parent (or otherwise legal representative) of the child. → Article 8(3) GDPR
Legitimate interest (paragraph 1(f))	The balancing of interests explicitly includes the best interests of the child (Article 3 UNCRC) as a primary consideration motivated. The data controller demonstrates how the rights and fundamental freedoms of the child (UNCRC) are adequately protected.

<i>GDPR</i>	
Article 7 GDPR	Conditions for consent
Transparency (paragraphs 2 and 3)	Insofar as the child is competent to give consent, the request for consent and also the notification of the possibility of withdrawing consent is comprehensible to them in all respects, given their age and their developing faculties (Article 5 UNCRC).
Freely given consent (paragraph 4)	→ Article 6(1)(b) GDPR

<i>GDPR</i>	
Article 8 GDPR → (Article 5 UAVG)	Conditions for children's consent in relation to information society services
Consent by children, parents or legal representatives (paragraph 1)	Persons aged 16 and above are authorised to give consent to processing of their personal data. Parents or legal representatives of persons under 16 are authorised to give consent to processing of their personal data on their behalf.
Reasonable effort (paragraph 2)	What is reasonable depends on the risk involved in the processing. Processing personal data of children is considered high-risk processing (→ Article 35(1) GDPR) and the starting point is that there is a high degree of certainty that a parent or legal representative has given consent for persons under 16 years of age. This is only different if there are specific circumstances that make it plausible that there is no of high-risk processing.

<i>GDPR</i>	
Article 9 GDPR	Special categories of personal data
Prohibition of processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a person, or data concerning health, or data relating to a person's sexual behaviour or sexual orientation (paragraph 1)	Personal data of children do not in themselves constitute a special category of personal data under Article 9 GDPR but the special categories mentioned may be particularly relevant for children given their vulnerable position and touch on specific children's rights. → Article 2 (UNCRC, non-discrimination), Article 6 UNCRC (personal development), Article 8 UNCRC (identity), Article 16 UNCRC (privacy), Article 24 UNCRC (health)
Express consent to the processing of personal data from a special category (paragraph 2 sub a GDPR)	→ Articles 7 and 8 GDPR

<i>GDPR</i>	
Article 12 GDPR	Transparency
Communication about the processing and the rights of data subjects in concise, transparent, understandable and easily accessible form and in clear and simple language (paragraph 1)	Information should be easily accessible and recognisable. The vocabulary, tone and style of language used should be appropriate and resonate with children. Information is presented in an inclusive manner and preferably in a variety of formats. Children's developing capacities are taken into account (Article 5 UNCRC) and children are heard (Article 12 UNCRC).

<i>GDPR</i>	
Article 17 GDPR	Right to data erasure ('right to oblivion')
Objection (paragraph 1(c))	→ Article 21 GDPR
Direct provision of information society services (paragraph 1(f))	A request for data erasure shall expressly take into account the best interests of the child and, in particular, the possibility that they have consented to the processing as a child (i.e. person under the age of 18) who was not fully aware of the risks associated with the processing and wishes to erase such personal data. → Article 8 GDPR → Recitals 38 and 65 GDPR

<i>GDPR</i>	
Article 21 GDPR	Right of objection
Determination of compelling legitimate grounds for processing which override the	The balancing of interests explicitly includes the best interests of the child (Article 3 UNCRC) as a primary consideration motivated. The data controller demonstrates how the rights and

interests, rights and freedoms of the data subject (paragraph 1)	fundamental freedoms of the child (UNCRC) are adequately protected.
Transparency notification (paragraph 4)	→ Article 12 GDPR

<i>GDPR</i>	
Article 22 GDPR	Online profiling
Prohibition of automated profiling if legal effect or otherwise significant effect (paragraph 1)	No absolute ban on online profiling of children, but the question of whether there is legal effect or significant effect needs an interpretation that does justice to the specific vulnerabilities of children. The best interests of the child take priority and online profiling for commercial purposes is not allowed (provided that a legal basis under Article 6 GDPR can be found for such processing). → Recital 71 GDPR → Article 6a(2) Audiovisual Media Services Directive → Article 4.1a(4) Media Act
Exceptions (paragraph 2)	The exceptions are interpreted restrictively with regard to children and will only be applied if it can be justified that it is in the best interests of the child. Safeguards must be appropriate, understandable and accessible to children. → Article 6(1)(a) and (b) GDPR

<i>GDPR</i>	
Article 24 GDPR	Accountability
Accountability (paragraph 1)	Data controllers must be able to demonstrate that they have adequately protected the rights and fundamental freedoms of the child (UNCRC) and justify how they have taken the best interests of the child (Article 3 UNCRC) as a primary consideration when designing their data processing processes.
Code of conduct (paragraph 2)	→ Article 40(2)(g) GDPR

<i>GDPR</i>	
Article 25 GDPR	Privacy by design and default
Likelihood and gravity of varying risks to the rights and freedoms of natural persons resulting from processing (paragraph 1)	Risks to children and their interests and rights are specifically identified.
Appropriate and effective measures and safeguards (paragraph 1)	Measures and safeguards should be appropriate, understandable and accessible to children.

<i>GDPR</i>	
Article 35 GDPR	Data protection impact assessment
High-risk processing (paragraph 1)	One of the high-risk criteria concerns data of vulnerable data subjects due to a greater power imbalance between the data

	subject and the data controller, which prevents the data subject, especially children, from consenting or objecting to the processing of their data. Processing children's personal data is reason to conduct a data protection impact assessment. Risks to children and their interests and rights are specifically identified. Children's right to be heard is respected (Article 12 UNCRC).
Assessment of risks to the rights and freedoms of data subjects (paragraph 7(c))	Risks to children and their interests and rights are specifically identified.
Codes of conduct (paragraph 8)	→ Article 40(2)(g) GDPR
Hearing involved (paragraph 9)	Children's right to be heard is respected (Article 12 UNCRC).

1.2.2 Protecting children from potentially harmful content

The Audiovisual Media Services Directive (AVMSD) contains provisions on the protection of children for video on demand services and video platforms. In the Netherlands, the directive has been implemented in the Media Act and the Media Decree. The rules regarding the protection of children from audiovisual content on video platforms that is potentially harmful to them are highlighted in the tables below. Harmful content must be distinguished from illegal content. Harmful content refers to images that are or may be harmful to children's physical, mental and moral development. Harmful content is not illegal content and can therefore simply be distributed, with the understanding that measures must be taken to prevent children from being exposed to content that is harmful to them. Illegal content, think incitement to hatred or terrorism or images of sexual abuse of children, is punishable by law and if an online platform has or reasonably should have knowledge of it, it should be removed (see Article 6 DSR). That said, illegal content for children can also be harmful content.

1.2.2.1 Media Act

One of the aims of the Media Act is to ensure that minors are protected from harmful content. In addition, the legislation requires media providers to handle the information they offer to children responsibly. The Audiovisual Media Services Directive⁶ has been implemented in the Media Act. In the elaboration, we limit ourselves to the protection of minors when offering video platform services (VPS) and video on demand services (VOS). Video platform services are digital services that offer user-generated videos to the public for which they have no editorial responsibility. They do rank the videos by automatic means and algorithms. Video on demand comprises audiovisual media services that provide audiovisual media offerings on individual request and at a time of choice. VPS, VOS and video uploaders established in the Netherlands⁷ with more than 500,000 followers fall under the supervision of the Media Authority (Article 3.29b and 3a.2 Media Act) and must join NICAM (Article 4.1 and 4.2 Media Act) and - if advertising is involved - the Advertising Code Foundation (Article 3.6 and 3a.4 Media Act). In addition to the Dutch Advertising Code, the Advertising Code Foundation has created relevant regulations for children, including the Children and Youth Advertising Code⁸, the Advertising Code for Online Games of Chance 2021⁹, and the Advertising Code for Social Media and Influencer Marketing.

⁶ <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32018L1808>.

⁷ <https://www.cvdm.nl/voor-medi makers/video-uploaders/nieuwe-regels-voor-video-uploaders/>.

⁸ <https://www.reclamecode.nl/nrc/kinder-en-jeugdreclamecode-kjc/>.

⁹ <https://www.reclamecode.nl/nrc/reclamecode-online-kansspelen-rok-2021/>.

<i>Media Law</i>	
Specific rules for video on demand	
Article 3.5b and 3.7(2)(a), 3.16(1), 3.17, 3.19b	Advertising is recognisable as such, does not use subliminal techniques and surreptitious advertising and does not advertise medical treatments. For sponsored offers, it is recognisable as such that and by whom it is sponsored. When mentioning the (title, name, brand of the) sponsored offer, the public may not be encouraged with specific commendations to buy or purchase the sponsored product or service. Product placement must be recognisable and is not allowed in respect of children under 12. → Articles 5, 6, 17(e) UNCRC
Specific rules video platform services	
Article 3a.3(1)	A provider of a video platform service based in the Netherlands shall apply a self-developed code of conduct in which appropriate protective measures are taken for minors against user-generated videos that may impair their physical, mental or moral development, in particular frightening, violent, pornographic images, images of drug use, as well as advertisements and other forms of marketing. For the most harmful content, such as gratuitous violence and pornography, the strictest measures will be taken. Appropriate measures see to the way content is organised (think of turning off autoplay for children by default). The code of conduct has clear objectives and there is regular, transparent and independent monitoring and evaluation of the measures. Moreover, there are effective enforcement mechanisms equipped with proportionate sanctions. To ensure sufficient support among stakeholders, children are also heard. → Articles 5, 6, 12, 17(e), 39 UNCRC → Article 4.2(2)(a) Media Act → Article 3a.3(4) Media Act → Article 3a.5 Media Act → Article 6a(1) AVMSD → Article 28b(1), (2) and (3) AVMSD
Article 3a.5	Advertising is recognisable as such, does not use subliminal techniques and surreptitious advertising. The VPS informs users in a clear manner about advertising in (user-generated) videos. In the case of children, the way of informing should be adapted to their age in a way that it is also recognisable and understandable for them that it is an advertisement. → Articles 5, 6, 17(e) UNCRC
Protection of minors by VPS, VOS and large video uploaders	
Article 4.1a	Children under 16 will not be shown or heard audiovisual images that could harm their physical, mental or moral development. This could include images that arouse fear, show or justify violence, attract or condone the use of drugs, alcohol or tobacco products, and sexually explicit images. The most harmful content (e.g. gratuitous violence and pornography) is made inaccessible to them.

	If the media services need to process children's personal data for the implementation of the provision (e.g. to carry out age verification), it will not be used for commercial purposes. → Article 6, 17(e) UNCRC
--	--

1.2.2.2 (other) right to advertise

There are also specific rules on advertising and promotion of games of chance aimed at minors. Among other things, it is prohibited to advertise online games of chance specifically aimed at children (and young adults).¹⁰

Advertising code for online gambling

The ROK contains specific safeguards for the rights of minors, considering the advertising of online gambling. For example, the code identifies minors as a vulnerable group of persons and, among other things, prohibits the use of merchandising aimed at minors. The code also states that advertising for online gambling should not reach an audience that is more than 25% minors and young adults combined.¹¹ It should be noted that there is a ban on offering online gambling services to children and young adults and gambling advertising may not be directed at them (see section 3.2.3.2).

<i>Online Gaming Advertising Code (ROK)</i>	
Article 6(3)	Advertising for online games of chance clearly and prominently states the minimum age to participate.
Article 6(4)	Online gaming providers do not use merchandising on or any other mention of their brands or logos on or near products or services specifically aimed at minors and young adults.
Article 6(5)	Advertising for online games of chance uses include no: sub a: Persons of a certain age; sub b: fantasy characters that specifically appeal to young people; sub c: athletes, other role models; sub d: conduct.
Article 9(2)	Advertising for online games of chance on billboards, swanks, bus shelters and mupis and objects with a similar purpose is prohibited within sight of educational establishments aimed at teaching minors or young adults, amusement parks, playgrounds, addiction centres and hospitals.
Article 9(3)	Advertisements for online games of chance shall not reach audiences that are more than 25% minors and young adults combined. The reach is determined over a representative measurement period determined according to the concrete circumstances of the case.
Article 9(4)	The prohibition in Article 9 Paragraph 4 does not apply if in a concrete situation an audience is reached that consists of more than 25% minors and young adults, if this happens unintentionally and if this is unexpected on the basis of the reach figures of the medium concerned.
Article 9(6)	Advertising for online games of chance, even outside the cases included in this article, does not target minors and young adults in terms of its distribution.
Article 9(7)	Advertising for online games of chance aimed at vulnerable groups of persons other than minors and young adults is also prohibited through media (including non-linear television services, print media, websites and social media) specifically targeting such vulnerable groups of persons.

¹⁰ Usually persons aged 18 to 25.

¹¹ Advertising Code Online Games of Chance article 9.3.

Article 9(9)	In advertising where the use of personal data or otherwise allows the recipients to be selected individually or by characteristics, indicators and/or filters should be used where possible to exclude vulnerable groups of persons. No further use should be made of characteristics belonging to those of vulnerable groups of persons.
Article 10(2)	Notwithstanding Article 6(5)(c), professional athletes and professional teams may be sponsored, with the exception of individual youth athletes and professional teams consisting predominantly of minors. To avoid misunderstandings, the ROK applies in full to the use of images of such sponsorship in advertising by the online gaming provider.
Article 13(1)(c)	In every single recruitment and advertising activity and in every (social) media account of the online gambling provider, the following information will be provided immediately and visibly or audibly: online (on websites, e-mail and social media) the warning that the content should not be shared with minors and young adults.

Children and Youth Advertising Code

<i>Advertising code for online gambling (ROK)</i>	
Article 1	Advertising aimed at children shall not contain anything in words, sounds or images that mislead children in any way about the possibility and characteristics of the product offered.
Article 2	Advertising aimed at children must not cause them moral or physical harm and must therefore meet specific criteria for their protection.
Article 3	Advertising aimed at children should not suggest that having or using a particular product gives them a physical or social advantage over other children, nor that not having a particular product leads to the opposite effect.
Article 4a	Regarding advertising in (youth) magazines or other printed matter with a reach of more than 25% among children, the word "advertisement" in 12-point letters should be placed above each advertisement (including the so-called advertorial).
Article 4b	Advertising on radio and television shall be clearly separated from the rest of the programme offer by optical and/or acoustic means. → Article 11 NRC.
Article 5	In the case of advertising aimed at children made visible on (= banner) and/or via (= pop-up) a website, the advertisement shall be provided with a clear indication of the word "advertising" or "ad", perceptible at a single glance. If an advertisement is smaller than 150 x 50 pixels, the abbreviation "adv." may be used. The provisions of this article also apply to banners and pop-ups in social media. If an advertisement contains a hyperlink, the page made visible by this hyperlink shall not contain any statements contrary to this code. Advertisements in posts and also other advertisements, not being banners and pop-ups, in social media used by children shall be clearly recognisable by optical, virtual and/or acoustic means appropriate to children's comprehension. Advertising in a virtual world in which children are present shall be clearly recognisable by optical, virtual and/or acoustic means that are appropriate to children's comprehension. (In-)Game advertising shall be clearly recognisable and distinguishable from the game by optical, virtual and/or acoustic means

	appropriate to the children's comprehension. (In-)Game Advertising directed at children should state clearly and unambiguously in the game and before the game can be started that the game, or parts thereof, is advertising and for which advertiser. An advertiser may not directly encourage children to advertise on behalf of the advertiser.
Article 6	In the case of advertising aimed at children via e-mail, each advertisement in the e-mail shall bear a clear indication of the word "advertisement" or "ad", which is visible at a glance. If an advertisement is smaller than 150 x 50 pixels, the abbreviation "adv." may be used. If the e-mail itself is the advertisement, the statement should be placed at the top of the body.
Article 7	In the case of advertising aimed at children via SMS, the SMS should have a clear, at-a-glance indication of the word "adv."
Article 8	It is prohibited to distribute or cause to be distributed unaddressed or advertising material addressed to children that can reasonably be considered to cause harm to the mental health of children.
Article 9	In a distance contract (other than teleshopping), the seller or service provider must encourage a child to obtain parental consent to enter into a contract. The seller or service provider must take all measures that can reasonably be expected of him to ensure that such consent has been given.
Article 10	Tele-shopping should not encourage children to enter into contracts to buy or rent products.
Article 11	The appearance in advertising in audiovisual media of persons who, on the basis of their participation in audiovisual programmes, can be deemed to have authority or trust with children is prohibited.
Article 12	When collecting personal data from a child, every effort should be made to inform the child and/or his or her parent of the purposes for which such data are processed. Where commercial child-oriented material is used or data of a child is otherwise knowingly collected, the information referred to above should be clear, easily accessible and understandable to a child. If, pursuant to law, a certain type of processing of personal data of a minor/young person under 16 requires consent, a parent/guardian must give such consent. When playing a game, offering a prize or any other activity with a sales promotion purpose, a child should not be required to disclose more personal data than is strictly necessary for that purpose.
Article 13	Advertisements for telephone information services of an erotic or pornographic nature or implicitly or explicitly referring to services of that nature shall not (partly) be aimed at, or use, minors. Advertising shall not directly or indirectly encourage minors to use these information services, nor shall such advertising contain any reference to minors.
Article 14	It is not allowed to make offers to consumers whom the telemarketer (the person engaged in telemarketing in an executive sense) knows, could know or should know are minors. → Article Code Telemarketing

Social Media and Influencer Marketing Advertising Code

<i>Social Media and Influencer Marketing Advertising Code</i>	
Article 5	If advertising via social media is aimed at children, the Children and Youth Advertising Code applies in full alongside this Code and the NRC.

1.2.3 Other conditions for digital services accessible to children¹²

1.2.3.1 Agreements entered into by children

By law, children (persons under the age of 18) may only enter into an agreement if they have the consent of their legal representative(s).

<i>Civil Code 1</i>	
Article 234(1) and (2)	Children are capable of performing legal acts, provided they have permission from their parent or legal representative. Digital services will therefore have to build in an option for parental control, where parents can grant consent. This consent can only be granted for a specific legal act or purpose. → Article 5 UNCRC → Protecting children from unfair commercial practices (parental control of restriction on spending by children)
Article 234(3)	This consent is presumed to have been granted to the child if it concerns a legal act in respect of which it is customary for minors to perform it independently given their age. It cannot simply be assumed that a minor has parental consent to play an online game. Furthermore - to the extent parental consent can be assumed - it is of course relevant that the child understands the conditions under which the agreement is entered into. This means that the information about the contract and its conditions must be able to be understood in a way that is customary for a child of the relevant age when entering into a contract. If the consent of the parent should not be assumed then refunds of costs incurred by minors as a result of an agreement with the service provider should be dealt with leniently. → Article 5 UNCRC → Article 6:230m of the Civil Code

1.2.3.2 Ban on provision of online gambling services

The Games of Chance Act stipulates that it is prohibited in the Netherlands to organise or offer games of chance to persons under 18 years of age. Adequate age verification will therefore have to be implemented to exclude children from online gambling services. 'Lootboxes' as part of a video game are not a standalone game of chance and are therefore not covered by gambling legislation.¹³ However, depending on how lootboxes are offered, they may be an unfair commercial practice towards children (see Consumer Law section).

¹² The Draft Cyber Resilience Act and the EU Toy Safety Directive were also consulted for the legal framework of the CRIA. However, these focus more on an actual product in relation to child protection and not online platform services.

¹³ <https://www.raadvanstate.nl/actueel/nieuws/@130150/202005769-1-a3/>.

<i>Gaming Act</i>	
Section 31k(2)(a)	It is not allowed to offer online gambling services to children. Adequate age verification should ensure that children cannot access online gambling services. → Articles 5, 6, 31 and 32 UNCRC → Protecting children from unfair commercial practices (misleading or aggressive commercial practices in the form of gambling-like design strategies, e.g. casino games and loot boxes)

Since online gambling services may not be offered to children, recruitment and advertising of online gambling services may not be targeted at children. For the sake of completeness, we mention here that the latter also applies to young adults.

<i>The Decree on recruitment, advertising and addiction prevention for games of chance</i>	
Article 2(3)	Licence holders may not direct their advertising to socially vulnerable groups of persons. Vulnerable groups of persons are, in any case, understood as minors persons and persons displaying characteristics of risky gaming behaviour.
Article 2(4)(a)	Gambling advertising should not target people between 18 and 24.

1.2.3.3 Consumer law

Legal obligations in consumer law stipulate that a digital provider must be transparent to users in various ways so that consumers can make an informed decision on whether to enter into a transaction. This also ensures consumer confidence in a digital service. Consumer law requires transparency on all aspects of a transaction. This means, for example, that the provider of a digital service must be clear about the costs of or in apps or games. With children, there is an additional obligation under the UNCRC to provide all such information in a way that is recognisable, accessible and understandable to children when they have the opportunity to enter into online contracts. This is extra relevant when parental consent to enter into contracts is assumed to be implicit, because it is common for children of a certain age to enter into a certain contract (see above 'Contracts entered into by children'). In that case, therefore, the fulfilment of information obligations¹⁴ to children will have to be in line with what children of the relevant age understand (Article 5 UNCRC). Furthermore, based on consumer law, providers have a greater duty of care towards children because they are considered vulnerable consumers. The latter is the case under the Unfair Commercial Practices Act. The ACM has published guidance on unfair (misleading and aggressive) commercial practices that also addresses the protection of children.¹⁵

Article 6:193c of the Civil Code	Children are more likely to be the subject of a misleading commercial practice than adults. When presenting information,
----------------------------------	--

¹⁴ Article 6:230m BW.

¹⁵ <https://www.acm.nl/nl/publicaties/voorlichting-aan-bedrijven/acm-leidraad/leidraad-bescherming-online-consumer/rules-over-in-game-sales>.

	digital services accessible to children will have to take into account what is recognisable, understandable and accessible to them. It should also be taken into account that the ability to recognise or critically reflect on advertising is often still lacking in children, which means that misleading commercial communications are more likely to occur. Examples of misleading commercial practices for children include: - Using virtual currency in apps or games without directly communicating the actual value in euros; - Presenting games as "free" when the game cannot be played in a way that can reasonably be expected without making in-app purchases or are based on an advertising model and processing a lot of personal data as a "means of payment"; - Hiding marketing in a digital service (e.g. no clear distinction for children between gameplay/non-commercial content and commercial messages); - Hidden or misleading advertising by influencers (even if it is mentioned that advertising is taking place, it may not always be recognisable or understandable to children / children may feel a personal connection with influencers (parasocial friendship) making them more impressionable by influencers); - Failure to clearly communicate what children can expect in terms of content and gameplay in games that are still in development ('early-access games'); - loot boxes where the chance of winning is not clearly stated or the prize (e.g. by using virtual currency is not clear (assuming children - given their age - are allowed to purchase loot boxes and have the ability to understand what loot boxes are and how they work); - (Other) dark patterns of a misleading nature (e.g. 'subscription traps'. → Article 5 and 32 UNCRC → Article 6:230m of the Civil Code → Media Act (protection of minors from harmful content)
Article 6:193i sub e BW	Children may be more likely to engage in an aggressive commercial practice than adults. Similar considerations apply here as for misleading commercial practices. Aggressive commercial practices for children include: - Using advertising to directly persuade children to buy advertised products or to persuade their parents or other adults to buy those products for them; - Games that merchants can reasonably expect to appeal to children that contain direct incentives to children to buy additional items in the game; - Direct encouragement to buy virtual gifts for or donate money to influencers and streamers on social media and video platforms; - Use manipulative strategies for offering microtransactions at certain critical moments in gameplay; - Inappropriately pressurising the gamer or user of online platforms with visual and auditory effects or by intrusive and continuous notifications; - Personalised commercial practices that specifically

	target consumer vulnerability (e.g. monetised matchmaking, manipulative targeted advertising and the use of algorithms that hold children's attention so they spend a lot of time on the service); - Pressuring children to buy a loot box (or other virtual items) by offering them at a point in the game when the child cannot make a considered choice (e.g. immediately after a lost game) (assuming children - given their age - are allowed to purchase loot boxes and have the ability to understand what loot boxes are and how they work) - (Other) dark patterns that inappropriately pressure children. → Article 5 and 32 UNCRC → GDPR (high-level data protection children) → Media Act (protection of minors from harmful content)
--	--

1.2.3.4 Digital Services Regulation (DSR)

The aim of the DSR is to make the responsibilities of digital service providers, such as online platforms, clearer and increase the safety of users online. In doing so, the DSR also takes particular account of (systemic) risks for minors. In addition, online platforms that primarily target minors must make special efforts to make their terms and conditions simple and understandable for minors.¹⁶ Online platforms are also required by the DSR to take appropriate and proportionate measures to ensure a high level of privacy, security and protection of minors within their service.¹⁷ Online platforms will additionally be prohibited from using "dark patterns".

DSR	
Article 20(3) and 21	The online platform accessible to minors has a child-accessible and also an otherwise child-friendly internal complaint system. The same applies to out-of-court dispute resolution options, where children should also be recognisably made aware of the possibility of involving a legal representative in case of a dispute. → Article 12 and 39 UNCRC → Article 28 DSR
Article 25	Online platforms accessible to minors specifically take into account the greater vulnerability of children in designing, organising and managing their online interfaces so that deception, manipulation or their ability to make free and informed decisions is disrupted or undermined. Children's abilities here may differ depending on their age or stage of development. → Article 5 and 32 UNCRC → BW (Protection of children against unfair commercial practices) → Article 28 DSR
Article 26	Online platforms accessible to minors shall indicate in a manner recognisable and comprehensible to children when advertising is shown by whom. This takes into account that advertising is usually only recognisable to children from the age of 8. [add ref]

¹⁶ Parliamentary letter on Digital Service Act and children's rights, p. 3.

¹⁷ Parliamentary letter on Digital Service Act and children's rights, p. 3.

	→ Articles 5, 6 and 17(e) UNCRC → Article 28 DSR
Article 27	When using recommendation systems, online platforms accessible to minors explain in language that is clear and understandable to children how they work, and provide tools that are useful for children to change their operation based on their preferences. In doing so, recommendation systems are safe for children at all times. → Articles 5 and 17(e) UNCRC → Article 28 DSR → Media Act (protection of minors from harmful content)
Article 28	Online platforms accessible to minors shall take appropriate and proportionate measures to ensure a high level of privacy, safety and protection of children within their service. What is appropriate or proportionate may depend on children's developing abilities. Advertising based on profiling (i.e. personalised ads based on behavioural information) is prohibited. To determine whether a user is a child, privacy-friendly alternatives are used that require processing of additional personal data. → Articles 5, 6, 16, 17(e), 19, 32, 34 UNCRC → GDPR (high-level data protection children)
Article 34	When assessing systemic risks, very large online platforms specifically consider the (potential) risks to children and their rights when using online platforms. This specifically requested assessment of risks distinguished within the online risk classification for children's physical and mental health, physical, mental, cognitive and moral development, well-being and rights. Among the particular factors considered in the risk assessment, namely algorithmic (recommendation) systems, content moderation systems, general conditions, selection and display of advertising and data-related practices, the risks to children are explicitly determined. → Articles 3, 5, 6, 16, 17(e), 19, 32, 34 UNCRC → Article 25-28 DSR → GDPR (high-level data protection children) → Media Act (protection of minors from harmful content)

Article 35	Very large online platforms take reasonable, proportionate and effective risk mitigation measures in view of the risks to children and their rights, with the impact of those measures monitored as part of the CRIA and measures adjusted as necessary. Measures may include implementing age verification to provide a digital service specific to children's age and development, providing opportunities for parents to supervise their children depending on their developing abilities when using digital services. 'Developing abilities' partly means that parental supervision tools are more suitable for young children. There are child-friendly and age-appropriate tools on the online platform for children to report abuse and get support if they experience abuse or other problems. Relevant information and age-appropriate settings are recognisable, understandable and accessible to children at all times. For settings, the child-friendly and age-appropriate option is selected by default. In that context, particular attention is paid to the design of online interfaces, general terms and conditions, content moderation procedures, algorithmic (recommendation) systems and advertising systems. → Article 3, 5, 6, 16, 17(e), 19, 32, 34 UNCRC → Article 25-28 DSR → GDPR (high-level data protection children) → Media Act (protection of minors from harmful
------------	---

1.2.3.5 Digital Markets Regulation (DMR)

The DMR aims to promote competition in digital markets and counter possible abuse of power by large digital platforms. In addition, the DMR also aims to protect users of the very largest online platforms.¹⁸ While the DMR does not contain specific articles of law relating to minors, it does establish a required higher level of protection for children's personal data.

<i>DMR</i>	
Recital 38	Children deserve specific protection with regard to their personal data, for commercial communications or user profiling. Protecting children online is an important objective of the Union and should be reflected in relevant Union legislation.

1.2.4 Conditions for offering products (online)

If the digital service, or any part of it, consists of the remote sale of products, it should be ensured that children cannot buy products that are harmful to them. This includes, in particular, the use of

¹⁸ <https://www.internetconsultatie.nl/uitvoeringswetdma/>

b1#:~:text=On%201%20November%202022%20is,for%20the%20most%20all%20online%20platforms.

an age verification system to provide a higher degree of certainty in determining the age or age group of an individual.¹⁹ More generally, it should be taken into account that children are in principle not allowed to enter into contracts independently (see chapter 3.2.3).

1.2.4.1 Ban on (online) sale of alcohol and smoking goods

<i>Alcohol Act and Decree</i>	
Alcohol Law	
Article 20(1)	Prohibition on selling alcoholic beverages to a person under 18.
Article 20a	Obligation to operate age verification system to prevent the sale of an alcoholic beverage to a person under 18.
Alcohol Decree	
Article 5.1	In every distance sale, before the conclusion of the contract with an active act of the buyer, it is established that the buyer is 18 years or older. In addition, it shall be established whether the person to be delivered is 18 or older.
Article 5.2	The remote seller provides a concrete description of how it is ensured that: - The person being supplied is 18 years of age or older, - That delivery is made only to the address of the consignee or distribution point, - The operating procedure is known and understood by those working under the responsibility of the vendor, and - An annual assessment of the implementation of the obligation under section 20a subsection 1 under b Alcohol Act is carried out (subsection 1, under a-d). The concrete description is up to date at all times (paragraph 2)
Tobacco and tobacco products act, decree and regulation	
Tobacco and tobacco products act	
Article 8(1)	It is illegal to sell tobacco products to a person under 18 years of age.
Article 9a(2)(d)	Remote sales of tobacco products, where not prohibited, should be subject to an age verification system.
Tobacco and tobacco products decree	
Article 1.1	The age verification system electronically establishes the age of the buyer. Note: A more privacy-friendly alternative is to establish whether a person has reached the minimum age. → Article 16 UNCRC
Article 5.6(2)	The age verification system establishes at the time of distance selling in the Netherlands that the buyer is 18 years or older.
Tobacco and tobacco products regulation	
Article 5.1(1)(f)	The seller shall prepare a description detailing the details and

¹⁹ Within today's digital markets, the following two standards are mainly used for age verification systems:
<https://standards.ieee.org/ieee/2089.1/10700/>
<https://www.iso27001security.com/html/27566.html>

	operation of the age verification system. With children in mind, this should establish whether the operation is understandable, recognisable and accessible to them. There should also be the possibility for age-appropriate reporting of problems with the functioning of the age verification system. → Articles 5, 12 and 39 UNCRC
Article 5.2	The age verification system reliably and unambiguously establishes the age of the purchaser. Note: A more privacy-friendly alternative is to reliably and unambiguously determine whether a person has reached the minimum age. → Article 16 UNCRC

1.2.4.2 Ban on (online) sale of weapons

Children are not allowed to own or obtain weapons within the meaning of the Weapons and Ammunition Act. In addition, an amendment to the Weapons and Ammunition Act to implement the Action Plan on Weapons and Youth,²⁰ which proposes, among other things, to prohibit the (online) sale of legal knives to children.²¹

2. Relationship of CRIA to other relevant guides

A CRIA is closely related to a number of other guidelines, guidance documents, review/consideration frameworks and impact assessments, including the Data Protection Impact Assessment (DIA), often also called the Data Protection Impact Assessment (DPIA). In addition, a CRIA also interfaces with the Fundamental Rights and Algorithms Impact Assessment (FRAIA). The tool enables an interdisciplinary dialogue by those responsible for the development and/or deployment of an algorithmic system.²² The CRIA will refer to such tools in several sections and thus builds on Age Appropriate Design Codes and standards (section 4.1.), FRAIA (section 4.2.), DPIA checklist AP (section 4.3.), UNICEF CRIA (section 4.4.) and Fair and Fact- Principles (section 4.5.).

2.1 The Dutch Child Rights Code and other 'age appropriate design' initiatives

The Children's Rights Code consists of 5 principles with practical examples that designers and developers can use to ensure children's fundamental rights in digital services. The principles are as follows:

1. Put the best interests of the child first;
2. Communicate with children at their level;
3. Involve children and their parents/carers;
4. Avoid a design harmful to children;
5. Estimate risks to children through a DPIA/FRAIA/CRIA.

Conducting a CRIA is enshrined in the 5th principle of the Children's Rights Code, following Article 3 UNCRC.

Similar initiatives exist in the European Union, viz:

²⁰ <https://www.rijksoverheid.nl/documenten/rapporten/2020/11/11/tk-bijlage-actieplan-wapens-en-jongeren>.

²¹ See also the accompanying Letter from the Minister of Justice and Security and the Minister for Legal Protection to the House of Representatives: <https://open.overheid.nl/documenten/ronl-0ce563e0-ebb5-49ac-9820-0eac071a813a/pdf>.

²² <https://open.overheid.nl/documenten/ronl-c3d7fe94-9c62-493f-b858-f56b5e246a94/pdf>.

- Swedish Guidance on Children's Rights Online, 2020 (Sweden);
- Age Appropriate Design Code, 2020 (United Kingdom);
- Fundamentals for a Child Oriented Approach to Data Protection, 2020 (Ireland);
- CNIL Recommendations for Protecting Children Online, 2021 (France);
- UK ICO Children's Code UX Design Guidance, 2022 (United Kingdom).

2.2 FRAIA

In 2021, the Ministry of the Interior and Kingdom Relations (BZK), in cooperation with Utrecht University, published the Human Rights and Algorithms Impact Assessment (FRAIA).²³ The FRAIA maps the social and legal risks about the use of algorithms by governments. In doing so, the assessment looks specifically at the impact of the algorithm to be deployed on human rights.

The FRAIA was created in response to the Surcharge Affair and the House of Representatives' desire to get a better grip on algorithmic applications. Through 57 open-ended questions, the tool encourages a measured discussion between relevant parties on the impact of the algorithm. The FRAIA refers to a number of manuals used in drafting the questions, such as the Handreiking non-discrimination by design²⁴, Ethical Guidelines Artificial Intelligence of the European Commission²⁵, the Toetsingskader Algemene Rekenkamer²⁶, the Integral Consideration Framework for Policy and Regulation²⁷, the Code Goed Digitaal Openbaar Bestuur²⁸ and the DPIA checklist of the Personal Data Authority²⁹.

The FRAIA consists of four dialogue sections, answering the following main questions:

- Why is an algorithm deployed and what are its intended effects?
- What kind of algorithm is being developed and what kind of data is being used for this?
- How is the algorithm deployed and audited? And what is the role of humans in making decisions based on algorithm outcomes?
- What impact does the algorithm have on fundamental and human rights? And do the intended effects of the algorithm outweigh the degradation of fundamental and human rights?

On 11 May 2023, the combined EU committees of the European Parliament approved an amendment to the draft AI Act (Draft AI Act) to require a human rights impact assessment (aka: Fundamental Rights Impact Assessment FRIA) for algorithms to include high risk.³⁰ The amendment aims at human rights and public values to play a more prominent role in the development and deployment of these systems. Besides human rights, the FRIA should also consider the impact of AI systems on the environment. However, it is not yet certain that this amendment will be in the final version of the Draft FRIA.

2.3 DPIA checklist Personal Data Authority³¹

Article 35 GDPR makes it mandatory to carry out a data protection impact assessment (DPIA)

²³ <https://www.rijksoverheid.nl/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algorithms>.

²⁴ Ditch, B. van der, Keymolen, E., Noorman, M., Weerts, H. J. P., Wagenveld, Y. & Visser, B. (2021). *Handbook on non-discrimination by design*. Central government.

²⁵ High Level Expert Group on AI (2019), Ethical Guidelines for Trusted Artificial Intelligence, Brussels: European Commission 2020.

²⁶ Audit Service Rijk (2021), General Court of Audit's review framework, 2021.

²⁷ Min Justice and Security (2022), Integral Assessment Framework Policy and Regulation.

²⁸ Meijer, A. et al (2021), Code Good Digital Public Administration.

²⁹ Personal Data Authority (2023), DPIA checklist.

³⁰ Article 29a Draft AI Regulation.

³¹ Personal Data Authority (2023), DPIA checklist.

when a processing operation is likely to present a high privacy risk. This risk may include the nature, scope, context and purposes of a processing operation. Conducting a DPIA should include identifying the purposes of data. Those purposes may also be relevant to the choices around the deployment of the algorithm as such.³² In addition, the Personal Data Authority (AP) has released a list of cases in which a DPIA is mandatory.³³ Such a DPIA will be necessary when deploying many algorithmic systems, especially when such deployment implies the processing of personal data.

2.4 UNICEF Children's Rights in Impact Assessment

The Children's Rights in Impact Assessment³⁴ is a guide by UNICEF that supports companies in assessing their policies and processes related to children's rights. The manual includes criteria that companies can use to assess their processes to analyse the impact on children's rights. Whereas the CRIA focuses on the impact of digital products and services, UNICEF's manual has a much broader scope and looks at all potential processes within a company that could harm children. UNICEF will develop a model CRIA for digital services in 2023/24.

2.5 The Fair and Fact principles

The FAIR and FACT principles assume that the use of big data only contributes to a better society for all when it is developed with important public values in mind.³⁵ The FAIR principles concern traceability, accessibility, interoperability and reusability. The FACT principles concern fairness, accuracy, confidentiality and transparency.

³² <https://open.overheid.nl/documenten/ronl-c3d7fe94-9c62-493f-b858-f56b5e246a94/pdf>.

³³ Official Gazette, 27 November 2019, No 64418.

³⁴ UNICEF (2013), Children's Rights in Impact Assessments.

³⁵ <https://open.overheid.nl/documenten/ronl-c3d7fe94-9c62-493f-b858-f56b5e246a94/pdf>.