THE ONLINE SAFETY ACT

A comparative legal analysis of the provisions for children

December 2023

Photography: Ron Lach

fieldfisher

5RIGHTS FOUNDATION

Introduction

The UK Government aims to make the country "the safest place in the world to be online",[1] in particular for children. Adopted in 2020, the Age Appropriate Design Code (AADC, or Code) set a high bar for children's privacy and safety by design and by default, across all online services they are likely to access. Whilst the Code was the first of its kind, it reflected a "global direction of travel" for implementing and enforcing children's rights online.[2] Three years down the line, the Online Safety Act (OSA)[3] further adds to this legal framework, seeking to ensure online services are safe by design and take particular account of children's additional rights, needs and vulnerabilities.

Whilst the Code regulates children's privacy (seeking to limit from the get-go the processing of children's data, and thus their exposure), and the Online Safety Act addresses content and online harms, both focus on corporate responsibility for outcomes and due diligence processes. Both place duties on tech companies to focus on how children use their services and ensure the best outcomes for children. Risk assessment and mitigation, with specific attention to features and functionalities that put children at risk and can lead to harm, are a focus of both regimes.

When the AADC came into effect in September 2021, it brought about hundreds of design changes that have delivered real benefits to children in the UK and around the globe.[4] The OSA, with its clear categorisation of harms and mandate to the regulator to develop, implement and enforce detailed codes of practice to safeguard children, has the potential to supercharge this progress.

I am very grateful to the Tech and Data team at Fieldfisher for conducting this comparative legal analysis for 5Rights. It provides an overarching view of what the OSA adds for children, building on the established requirements of the AADC. It remains a first assessment, and what exactly the OSA will actually deliver will to a great extent be determined by Ofcom and its codes of practice. We hope, therefore, to soon be able to add to this analysis, and celebrate the promise of the OSA translating into a safer, better, digital world for children.

Leanda Barrington-Leach
Executive Director, 5Rights Foundation

[1] Michelle Donelan MP, Secretary of State for Science, Innovation and Technology, Press release: UK Children and adults to be safer online as world-leading bill becomes law, (October 2023)
[2] Elizabeth Denham CBE, Information Commissioner's Foreword to the Age Appropriate Design Code, (2020)
[3] Online Safety Act, (2023)
[4] Press release: 5Rights marks the second anniversary of the Age Appropriate Design Code, (September 2023)

Comparative legal analysis

Key points of convergence

- Like the AADC, the OSA recognises that children, defined as all under 18s, have the right to a higher standard of protection than adults.
- For both regimes there is a requirement to understand who the users of your service actually are, specifically with regards to age, by assessing whether children are "likely to access" it. The Information Commissioner (ICO) and Ofcom have commissioned collaborative research into age assurance.[5]
- With respect to both the AADC and OSA, responsibility is put upon companies to consider the user journey of their service and provide children with high levels of protection by design and by default.
- Both regimes require comprehensive up-front risk assessments and mitigation plans, which need to be regularly reviewed and updated. Performing a Data Protection Impact Assessment (DPIA) under the AADC and a children's risk assessment under the OSA will provide a comprehensive audit of the service offered and enable any risks to be better managed.
- Having transparent and easily accessible information available for users is pertinent to both regimes.
- With regard to enforcement, both regimes include substantive financial penalties.

Key points of divergence

- The purposes of the regimes are different, but complementary. The AADC focuses on privacy and data protection, limiting the processing of children's data in the first place, whereas the OSA focuses on online harms, and illegal and harmful content. Practically, the AADC focuses on how features and functionalities of online services affect children's privacy and the use of their personal data, whilst the OSA looks at the risks of harmful content available online and how features and functionalities of online services may enhance or create harm.
- Unlike the OSA, the AADC is explicitly grounded in the UN Convention on the Rights of the Child.[6]
- The scope of the OSA and the AADC is, to some extent, different. Whereas the AADC applies to all online services 'likely to be accessed' by children, the OSA regulates user-to-user and search services, as well commercial pornography websites, but the majority of its provisions apply to all services (not only those 'likely to be accessed' by children).

[5] Age Assurance research, ICO
[6] Convention on the Rights of the Child, United Nations

Additional requirements of the Online Safety Act

- As an Act of Parliament, the OSA includes additional measures, including mechanisms for Ofcom to lend its new information gathering powers to coroners investigating the death of a child.
- The OSA introduces new offences for the online world, including for encouraging or assisting serious self-harm, epilepsy trolling, sending knowingly false or threatening communications, and new sexual offences for revenge porn and cyber flashing.
- The OSA includes a legal requirement for age assurance to prevent children's access to pornography. Ofcom has begun to consult on its guidance[7] for services publishing pornographic content.
- The OSA requires a children's risk assessment looking at harms beyond those generated by the processing of personal data.
- The OSA adds new requirements regarding the terms of service, which need to detail how children are to be prevented from encountering primary priority content that is harmful to them.
- With regard to enforcement, the OSA provides for higher financial penalties as well imprisonment for senior management.

[7] Consultation: Guidance for service providers publishing pornographic content, Ofcom (5 December 2023)

Areas of consideration	Age Appropriate Design Code	Online Safety Act
Legal Status	Statutory Code (s123 Data Protection Act 2018)	Act of Parliament
Regulator with responsibility	Information Commissioner's Office (ICO)	Ofcom
Objectives		
	The AADC is rooted in the UN Convention on the Rights of the Child, and aims to safeguard children's privacy and protect their personal data when they access online services by requiring services to put the best interests of the child first when they are designing and developing apps, games, connected toys and websites that are "likely to be accessed" by children. The focus is on the age appropriate design of online services. This involves transparency and providing default settings which minimise data collection and use, whilst ensuring that children have the best possible access to online services. It also ensures that children who choose to change their default settings get the right information, guidance and advice before they do so, and restricts the use and sharing of children's data.	The OSA seeks to secure (among other things) that regulated services are: (1) Safe by design; and (2) Designed and operated in such a way that: a. A higher standard of protection is provided for children than for adults; b. Users' rights to freedom of expression and privacy are protected; and c. Transparency and accountability are provided in relation to those services.

	The AADC assumes that the online service provider is compliant with applicable UK Data Protection law (including the Data Protection Act 2018 and the UK GDPR (General Data Protection Regulation).	
Scope		
Territorial scope	Any online service provider offering services into the UK or monitoring behaviour of individuals in the UK.	Online services with "links" to the UK, including if the service has a significant number of users in the UK, or the UK is one of their target markets (or the only market). Having a "link" to the UK also relates to services that are capable of being used in the UK by individuals and there are sufficient grounds to suggest that people in the UK face a material risk of significant harm from user-generated content or search content.
Stakeholders in scope	Any provider offering online services "likely to be accessed" by children and/or offering connected toys. The possibility of a child accessing a service needs to be "more likely than not". The intention is that it covers "all services that children use in reality".[8]	"User-to-user services", "search services" and providers of commercial pornography. A "user-to-user service" means an internet service by means of which content that is generated directly on the service by a user of the service (including automatically generated content) or uploaded to or shared on the service by a user of the service, which may be encountered by another user, or other users, of the service. See OSA s3(1).

[8] 'Likely to be accessed' by children – FAQs, list of factors and case studies, Information Commissioner's Office

		Services will be categorised by the Secretary of State into Category 1 (regulated user-to-user service), Category 2A (regulated search service or combined service) or Category 2B (regulated user-to-user service with certain functionalities). The Secretary of State will make regulations to determine the "threshold conditions" in relation to Category 1, 2A and 2B services/search engines. Attention will be given to the number of users, functionalities of the user-to-user service/search engine, as well as other characteristics of that part of the service/search engine or relating factors. See OSA Schedule 11(1). Certain additional provisions apply only to services "likely to be accessed" by children. Services will be considered "likely to be accessed" by children where a children's access assessment concludes that: (1) It is possible for children to access the service or a part of it; and (2) The child user condition is met in relation to the service or its part, meaning that: a. There is a significant number of children who are users of the service/part of the service (significant in proportion to the total number of UK users); or b. The service (or part of it) is likely to attract a significant number of users who are children.

		Where a service provider fails to carry out a children's access assessment, the relevant service will be treated as "likely to be accessed" by children until the completion of the first children's access assessment or if, following the failure to carry out a children's access assessment, Ofcom determines that the service should be treated as "likely to be accessed" by children.
Material scope	Personal data of children in the context of the design (including the user journey) of an online service. The primary focus of the AADC is to ensure that a child's data is given the highest level of protection, that privacy by design and by default is implemented, and the functionalities and associated documents for the service are age appropriate.	Online harms, with a higher bar of protection for children. The OSA addresses the impact of the functionalities and features that affect activity such as the length of time a child uses a service and the impact such use might have on the level of risk of harm that may be suffered by children. It also has a clear focus on content, with provisions addressing: (1) "Illegal content", which relates to terrorism, child sexual exploitation and abuse, assisting suicide, threatening to kill, public order offences including fear or provocation of violence, harassment, supply of drugs and psychoactive substances, firearms and other weapons, assisting illegal immigration, human trafficking, sexual exploitation, sexual images (including revenge pornography), assisting crime and fraud (s59 and schedules 5-7); and (2) "Harmful content" – a category applying only to children – relating to pornographic content, or other material that does not meet a criminal threshold but promotes,

		encourages or provides instructions for suicide, self-harm or eating disorders, depicts or encourages serious violence and/or relates to bullying (s60-63). The OSA divides harmful content into types and there are stricter duties based on the severity: a. Primary priority: Content which is pornographic; encourages, promotes or provides instructions for suicide; encourages, promotes or provides instructions for an act of deliberate self-injury; or encourages, promotes or provides eating disorders (s61). b. Priority content: Content which is abusive and which targets race, religion, sex, sexual orientation, disability or gender reassignment; incites hatred against people with certain characteristics; encourages or promotes acts of serious violence against a person; bullying content; content which depicts real or realistic serious violence or injury against a person, animal or a fictional creature; which promotes or encourages a challenge highly likely to cause serious injury; or encourages a person to digest, inject, inhale a physically harmful substance or a substance in such quantity as to be physically harmful (s62). c. Non-designated: Content which presents a material risk of significant harm to an appreciable number of children in the UK.

Compliance requirements		
Risk assessments	Services must undertake a Data Protection Impact Assessment (DPIA) to assess and mitigate risks to the rights and freedoms of children who are likely to access a service which arise from data processing. A DPIA is a process to support organisations to: identify the nature, scope, context and purpose of processing; assess the necessity, proportionality and compliance measures of the processing; identify and assess risks to individuals; and identify targeted measures to mitigate those risks. A DPIA should assess compliance with the AADC, taking into account differing ages, capacities and developmental needs of child users. The DPIA must be completed before a service is launched. Organisations may choose to make their DPIA, or a summary of it, public.	In addition to an illegal content risk assessment, services "likely to be accessed" by children must undertake a children's risk assessment, identifying the possible harms and how those harms will be mitigated. The risk assessment must take into account the extent to which the design of the service, including its functionality, affects the level of risk of harm to children – (s11(6)(e) and (f)). There is a formal requirement under the OSA for summaries of risk assessments for Category 1 and 2A services to be made public. Risk assessments must be carried out within three months of the publication of Ofcom's risk profiles, and prior to making any significant change to the design or operation of a service.
Age assurance	Services must take risk-based approach to recognising the age of individual users and ensure they effectively apply the standards in the AADC to child users. This can be done through either establishing age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from the data processing, or	Age verification (defined as any measure designed to verify the exact age of users of a regulated service) and age estimation (meaning any measure designed to estimate the age or age-range of users of a regulated service) are amongst measures which may be taken by service providers to comply with online safety duties.

	applying the standards in the AADC to all users instead.	In accordance with the OSA, a service provider will only be able to conclude that it is not possible for children to access a service, or a part of it, if age verification or age estimation is used on the service with the result that children are not normally able to access the service or its part. The OSA explicitly requires services to use age verification or age estimation (or both) for two purposes: 1) To prevent children from encountering primary priority content that is harmful to children, which the provider identifies on the service; and 2) To prevent children from encountering regulated pornographic content. In these cases, service providers must use age assurance measures in such a way that the age checks are highly effective at correctly determining whether or not a particular user is a child. All online services in scope of the OSA will also need to reflect the use of age verification or age estimation technology in their terms of service (including information about the kind of technology, when it is used, and how it works). An additional duty – to keep written records of the types of age verification or age estimation used and the interactions between online safety and privacy, and to summarise them in a publicly available statement – applies in the context of preventing access to pornographic content (s82 OSA).

Terms of service	Documents need to be written in a clear and age appropriate manner. Policies and terms must be upheld, such as in relation to behaviour.	Terms of service need to be transparent and contain easily accessible information regarding child protection measures. The terms of service need to detail how children are to be prevented from encountering primary priority content that is harmful to them. They must be applied consistently.
Safety by design	The 15 interdependent standards of the AADC aim to make services embody a high level of privacy, and be safe for children, by embedding data protection by design and by default. Services must make the best interests of the child a primary consideration when designing and developing online services "likely to be accessed" by a child. Settings must be "high privacy" by default (unless there is a compelling reason not to); only the minimum amount of personal data should be collected and retained; children's data should not usually be shared; and profiling and geolocation services should be switched off by default. Nudge techniques should not be used to encourage children to provide unnecessary personal data, weaken or turn off their privacy settings.	The OSA mandates safety duties protecting children for services that they are likely to access. In addition to safety duties relating to illegal content, providers must operate a service using proportionate systems and processes designed to mitigate and manage the risks and impact of harm to: 1) Prevent children encountering, by means of the service, primary priority content that is harmful to them; and 2) Protect children in age groups judged to be at risk of harm from other content that is harmful to children (or from a particular kind of such content) from encountering it by means of the service – (s12(3) OSA).
Reporting	The AADC requires services to provide prominent and accessible tools to help children exercise their data protection rights and report concerns.	The OSA requires services to enable users and affected persons to easily report content which they consider to be illegal or harmful to children. Services and search engines will need to investigate the reported content.

	In addition to bringing a complaint to the service provider, affected individuals can make a complaint to the regulator.	The OSA has no independent complaints mechanism – services have discretion in how they address this requirement.
Record-keeping	GDPR requires providers to document compliance measures and maintain records of processing activities, including data categories, categories of data subjects, the purpose of the processing and the data recipients. An AADC DPIA provides a detailed record that must be kept, reviewed regularly and made available upon request to the regulator.	Category 1 and 2A services need to supply Ofcom with their risk assessments. A written record of risk assessments/compliance measures will need to be kept and reviewed regularly. Any significant change to any aspect of the design or operation of the service is subject to a risk assessment and needs to documented accordingly.
Deceased children	N/A Deceased children are not in scope of the AADC (due to the scope of data protection law covering the data of living individuals only).	Relevant services need to make it clear in their terms of service what their policy is with respect to how they will deal with requests from parents or guardians of a deceased child who want information about their child's use of the service. Service providers need to offer a dedicated helpline or similar service and provide details in their policies to explain to parents and guardians how they can easily obtain their child's information (s75 OSA). Ofcom may use its information gathering powers on behalf of the coroner, requiring a relevant person to provide them with information for the purpose of responding to a notice given by the coroner in connection with an investigation into the death of a child (s101 OSA).

Enforcement		
Fines	Maximum of £17m or 4% of an undertaking's total worldwide annual turnover, whichever is higher.	Maximum of £18m or 10% of qualifying worldwide revenue (Ofcom is to provide regulations in relation to how this is defined) (s85 OSA).
Imprisonment	N/A	Maximum of up to 2 years' imprisonment for senior managers (s138) where a service does not comply with an Ofcom enforcement notice in relation to specific child safety duties, or in respect of child sexual abuse and exploitation.

Please note the information in this document is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer for advice on any specific legal matters.