

May 2019

## Response to the ICO's draft code 'Age Appropriate Design: A Code Of Practice for Online Services'

The Digital Policy Alliance thanks the Commissioner for providing the opportunity to comment on the ICO consultation 'Age Appropriate Design: a Code of Practice for Online Services'.

The DPA's AVIS Group submitted a response to the initial call for evidence and we are pleased to see that the Commissioner has included many of the points that we made at that time.

We have continued to contribute to the work of the 5Rights Foundation and we fully support their response to the draft Code. In our response, we want to focus on the issues relating to Age Verification Systems and Certification; however, we continue to support and endorse the wider development of the Code.

We want to start by saying that the Draft Code is an outstandingly good piece of work by the Commissioner. Section 123 of the Data Protection Act 2018 set a tough brief for the Commissioner to issue standards of age-appropriate design of relevant information society services which are likely to be accessed by children. The Commissioner could have approached that task with a restrictive interpretation of that brief, instead she has chosen to take an open, ground-breaking and carefully considered view. We fully support that approach, which we hope is not diluted by ill-conceived lobbying from the Tech Sector to protect inappropriate commercial business models that, even if only inadvertently, exploit data provided freely and unknowingly by children.

### Age Verification Mechanisms (Standard 2)

There are 16 Code standards of age appropriate design for online services listed at the beginning of the consultation document, for information society services likely to be accessed by children. At the outset, we wish to emphasise the dangers inherent in the self-selection of date-of-birth by children, where they are able to pretend that they are older. These weak age gateways have become prevalent across information society services and social media.

The ICO may be interested to review what approaches can age-verify or age-estimate people under the age of 18, given that this code segments the under 18s into five age bands of 0-5, 6-9, 10-12, 13-15, 16-17 based on developmental stages.

There needs to be a review of what are the evidence points / data sets and their availability / penetration across the population. Are they accessible to all? For instance approximately one third of under 18s do not have a passport, with a high correlation to the C,D,E demographic. In Scotland the Young Scot card is issued for free to young people at senior school, this is not the case in England and Wales. There is not currently access to age or identity providers to other evidence data such as schools' data.

## Standards & Certification

In evidence to the Digital, Culture, Media & Sport Committee<sup>1</sup> before Parliament, the Director of Public Affairs for Snapchat conceded that their age gateway does not work (self-declared age) and claimed that the only way of doing this was likely to be some central verification system administered by governments. We disagree. The technological advancement of age verification, incorporating privacy protection makes it entirely possible to implement robust age verification solutions. The DPA was pleased to sponsor and lead the development of PAS 1296:2018 with the British Standards Institution. This Code of Practice for Online Age Verification lays down the framework for implementation of appropriate age verification controls – both for the age verification service providers, but also for the relying parties, merchants or website operators.

Whilst the PAS 1296:2018 provides a clear framework, where a specific use case dictates a layering of higher standards and protocols, these can also be incorporated into the draft Code's standards framework. The British Board of Film Classification (BBFC), for instance, has identified the very particular risks to privacy from weak data security measures when adults are entering age gateways in order to access online pornographic content. This has led to the development of a specific data security standard for that use case. To be fully effective, standards should be implemented in a consistent and mutually supportive manner – importantly within the framework for accreditation and standards set out in the Accreditation Regulations 2009 (SI2009:3155). This ultimately requires the oversight of the United Kingdom Accreditation Service of the certification bodies applying those standards.

We also note the emerging development of a standards framework under Articles 42 & 43 of the General Data Protection Regulation. Once the European Data Protection Board have fully implemented the provisions of supervisory control of that standards framework, it is our view that any age verification standards, including certification under PAS 1296:2018 ought to be brought within that supervisory framework – whilst noting that inevitably the provision of online age verification has to be both compliant with data protection principles and be operationally effective – it is important to ensure that standards do not address just one problem, and not the other.

We note the proposal that providers apply the standards in the Code to all users, unless there are robust age-verification mechanisms to distinguish children from adults. This is amplified later (e.g. Page 24) to require that those who choose to apply the standards to “only users who are children (and not to users who are adults),” can do so only if robust age-verification mechanisms are present ‘up front’ to confirm the age of each user.

We note that the consultation document recommends provision of “a child-appropriate service to all users by default, with the *option* of age-verification mechanisms to allow adults to opt out of the protections in the Code and activate more privacy-intrusive options if they wish.” There is a clear proposal that where only adults are likely to access a service so that the Code does not apply, a provider needs to be able to demonstrate this ideally by having *robust* age-verification in place as demonstrating the clearest evidence.

The Code strikes the right balance here, requiring online services to give children's data specific protection, without stipulating the mechanism of verification. Rather, the Code simply requires that this is done in a robust and effective way. This allows for the use of a number of existing options as well as for future innovation. It also allows companies who do not wish to establish which of the users are children to apply by default the Code's standards to all users, thereby ensuring the standards are applied to all children. The Commissioner is also right to state that data may be collected for age verification purposes but must not then be used for any other purpose.

---

<sup>1</sup> Snapchat's evidence to the Digital, Culture, Media, and Sport Committee's inquiry on Immersive and addictive technologies, March 2019

We welcome the commitment the Commissioner has made to “support work to establish clear industry standards and certification schemes to assist children, parents and online services in identifying robust age verification services which comply with data protection standards.” **Our recommendation is that *where a website appears to be targeted at children, but has content that is not age appropriate, then AV must be required for access either to the entire website or to pages where such content is contained.***

The DPA’s AVIS Group has been at the forefront of developing and demonstrating operational online AV solutions to Government officials and Parliamentarians that will help to ensure under 18s are not normally able to access online pornographic material (under Part 3 of the Digital Economy Act 2017). Group members include AV providers who can offer robust, effective, data-minimising and privacy-friendly solutions to allow a service to adults without regard to the Code, and are able to demonstrate that children cannot easily circumvent the age checks.

### Risk Based Approach

In our view, the Code would benefit from some additional statements about taking a risk-based approach. We appreciate that in certain circumstances, risk-based approaches may lead to ambiguity or borderline cases, but in our view, that ought not be a mechanism for avoidance. Instead, it should provide the flexibility to the application of the Code and proportionate enforcement.

There will, of course, be borderline cases. An online retail catalogue may provide images of lingerie on its website. Without stepping into the world of provocative and sexualised imagery, it is perfectly fair for such a website to provide plainly taken ‘thumbnail’ images of lingerie for adults on its website. Is that something that ought to be behind an age gateway? No doubt children will access those images – in much the same way as previous generations viewed mail order catalogues. There is, of course, a market for under garments and underwear for children – although there are already very strict rules in place about models and photography for that. It’s difficult to conclude that this age-inappropriate content might be required to be behind an age gateway, but only after the application of a risk-based and proportionate approach to enforcement.

Instead, we support an approach that requires online services to implement demonstrably robust age verification mechanisms if they do or have any of the following;

- (a) a large numbers of child users,
- (b) pose a particular risk to children,
- (c) process significant amounts of children’s data,
- (d) process particularly sensitive children’s data, or
- (e) make sensitive or impactful judgments on the basis of children’s data.

In our view, services that do not process a child’s data in these ways or for these reasons, or services that are demonstrably in the best interests of a child, many not require the same level of or any age verification, but must still comply with the other provisions of the Code.

### Summary

We have refrained from setting out views on all aspects of the proposed code. Other respondents, particularly the 5Rights Foundation that we have supported, will submit useful and practical suggestions on the drafting of the Code.

Overall, we wish to commend the Commissioner for an excellent piece of work and we look forward to implementation of it in due course. We are, of course, happy to assist and provide further evidence specifically on the technical feasibility, standards and privacy-protection associated with online age verification systems.