defenddigitalme response to the Age Appropriate Code of Practice consultation (stage two)

defenddigitalme is a call to action to protect children's rights to privacy. We are teachers and parents who campaign for safe, fair and transparent data processing in education, in England, and beyond. We advocate for children's data and digital rights, in response to concerns about increasingly invasive uses of children's personal information. The campaign is funded by an annual grant from the Joseph Rowntree Reform Trust Ltd.[1]

[1] More information about defenddigitalme https://defenddigitalme.com/about/

Summary

We welcome the opportunity this gives policy makers and industry to debate children's data rights and warmly support those aims to better inform children about their rights regards data protection and the aspects of the Code that aim to support better privacy.

We are pleased to see that the Code recognises that enforcement not only monitoring is a necessity, if change is to come, in saying '*where see harm or potential harm to children we will likely take more severe action against a company than would be the case for other types of personal data*.' We look forward to work such as from the findings[2] of the 2018 GPEN privacy sweep, known breaches,[3] and academics research[4] into privacy and data protection breaches, will result in ICO action to better support UK children's privacy protections.

Our key concerns on the development of the Code at the current time, mean that we cannot support the current ICO proposals for Age Verification. Insufficient attention has been given to the risks and benefits for children, which the ICO itself stated in the House of Lords Consultation on *Children and the Internet* in 2016, as we set out in more detail that follows.

We have further significant concern over the lack of clarity on territorial scope, content scope creep between the two consultations, and its implications for children among all Internet users, as well as for meaningful ICO enforcement.

There is

- unreadiness for the newness of the wide ranging implications since the Code basis (Clause 123) was not part of general GDPR preparations but only finalised in the UK, in the 6 months before GDPR became enforceable in May 2018.
- untested significant effects of the changes for children and wider users of ISS.
- uncertainty regards data processing over leaving the EU and its implications.[5]

The purpose of statutory Codes should be to explain the primary UK Data Protection legislation, the 2018 Act, and ensure processing is made more understandable. GDPR is intended to provide a consistent level of data protection. This Code appears to now try and go far beyond both of these remits, to create new 'desirable' statutory obligations, rather than better interpret and explain those which are already in the Data Protection legislation.

We recommend therefore that the ICO sets and publishes future review dates for further consultation on certain aspects of the Code and continues to consult.

We make reference to our response to the ICO Statutory Age Appropriate Code of Practice (Data Protection Act 2018) as, *the ICO stage one consultation*[6] and this as *stage two*[7].

[2] GPEN privacy sweep 2018 https://ico.org.uk/about-the-ico/research-and-reports/information-rights-research/
[3] VTech (The Register, 2018) https://www.theregister.co.uk/2018/01/18/innotab_kid_tech_still_vulnerable/
[4] "Apps targeted at children appear to be amongst the worst in terms of number of third party trackers associated with them" https://www.independent.co.uk/life-style/gadgets-and-tech/news/android-apps-google-study-data-privacy-facebook-amazon-oxford-university-a8599541.html with reference to Binns, R. et alThird Party Tracking in the Mobile Ecosystem (2018)
[5] Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection 19/01/2018 https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=611943
[6] Our 2018 Stage One ICO Age Appropriate Design Code Consultation Submission https://defenddigitalme.com/wp-content/uploads/2018/09/defenddigitalme_AACOP_ICO_FINALV1.1.pdf
[7] Stage two ICO Age Appropriate Design Code Consultation https://defenddigitalme.com/wp-content/uploads/2019/06/age-appropriate-design-code-for-public-consultation1-1.pdf

Scope creep

Our primary concern is now the scope creep from the *ICO stage one consultation* in Autumn 2018 to this second stage of consultation. We understand that the Data Protection Act 2018, affords the Commissioner discretion to set such standards of age appropriate design "as she considers to be desirable", having regard to the best interests of children, and to provide such guidance as she considers appropriate. As we understand it, this opinion based 'desirable' scope, should still be in the scope of the role, rather than as the ICO an individual.

However, the newly stretched scope goes far beyond the original list the Government provided the Commissioner to take into account, and beyond the published ICO strategy 2017-21 to focus on children's privacy[8]. We believe the 'best interests' on page 20, and the areas of focus that were listed in the Stage One consultation, should remain only those that fall within the ICO Data Protection remit.

There has been a significant shift in the tone and emphasis of proposals, as well as the breadth of the scope between the *stage one consultation* to now. We also sense the Code has lost the focus of its basis in Data Protection law under the UK Data Protection Act 2018 and Regulation (EU) 2016/679 of the European Parliament and of the Council, (GDPR).

The consistent elements of the ICO approach to data protection and children in law, and which appear in the new draft Code proposals, supporting its original areas of design and topics suggested by the government in the Stage One consultation, all remain strong, including, from the new topic areas what we have separated into Group A and Group B:

(Group A)
(3) Transparency, and education,
(6) Default Settings (regards privacy)
(7) Data minimisation
(8) Data sharing
(15) Data Protection Impact Assessment
(16) Governance and Accountability

[8] ICO 2017-21 Draft Regulatory Action Strategy
https://defenddigitalme.com/wp-content/uploads/2019/06/ico-draft-regulatory-action-policy.pdf

Extract from ICO Stage one consultation, the government recommended topics to consider.

These are as follows:

- default privacy settings,
- data minimisation standards,
- the presentation and language of terms and conditions and privacy notices,
- uses of geolocation technology,
- automated and semi-automated profiling,
- transparency of paid-for activity such as product placement and marketing,
- the sharing and resale of data,
- the strategies used to encourage extended user engagement,
- user reporting and resolution processes and systems,
- the ability to understand and activate a child's right to erasure, rectification and restriction,
- the ability to access advice from independent, specialist advocates on all data rights, and
- any other aspect of design that the Commissioner considers relevant.

We welcome for example in the new proposals (8) the reinforcement of data protection law that commercial re-use is not a compelling reason for data sharing using legitimate interests, (10) the recommendation that monitoring a child must be obvious, and that (9) geolocation tracking should be off by default and enable easy-to-understand active choices.

The summary of the Code standards where they deviate away from data protection, are more problematic within the ICO remit, insofar as where they reach beyond data protection law in particular in (11) in which the Code appears to venture into the realm of making recommendations on contextual tagging, and on the 'general approach' regards children's health and well-being, promoting content, and behaviours:[9]

(Group B)
(1) Best Interests of the child (where this strays into broad design, beyond data protection)
(2) Age Appropriate Application
(4) Detrimental use of data (since this strays into vague notions of wellbeing, not data)
(6) Default Settings (beyond privacy high and data protection settings, such as recommendations on appropriate technology for user ID on multi-use devices)
(9) Geolocation
(10) Parental Controls
(11) Profiling (insofar as where it goes beyond the scope of the aspects of GDPR Recital 71)
(12) Nudge techniques
(14) Online Tools
plus
(13) Connected Toys and the IoT (given the active DCMS consultation)

With regards to, the 2019 DCMS consultation regarding consumer Internet of Things security, sees some overlap and potential conflict. For example, the standard it references (ETSI TS 103 645 V1.1.1 (2019-02))[10] applies only to IoT products primarily intended to be employed in manufacturing. *Other industrial applications and healthcare* ***are not in scope*** -- but in this Age appropriate Design Code of Practice, "fitness bands" would appear to be *in* scope, and there might be confusion in the public's mind what should and should not fit

[9] With the greatest of respect, these topics are beyond ICO staff core capabilities and capacity; recommendations for them, even within a DPIA, should not stray into this territory which it cannot regulate (page 65). The wording needs narrowed.
[10] IoT https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

where. The ICO Code of Practice makes no requirement on data anonymisation in IoT, which the ETSI standard does in Provision 4-10.2.

Recommendation: Transition, trial, and testing success

In order to get a deliverable and enforceable Code into practice, we recommend either a narrowing of the scope to Group A, or at the very minimum, a two-phased implementation, with a rolling review, as permitted in Clause 123(5), (6) and (2).

We note that there is no way for the ICO to measure the effects or otherwise of the aims of the Code, or to provide some quantitative measures of success, or harms, for a set of broad standards that are qualitative, and not neutral in either their politics or technology.

The LEGO group stage one response[11], also proposed testing on communications:

> There is also an opportunity here for the ICO to begin to explore the possibility of testing certain communication techniques with children. Ideally a chosen method employed by a business should be underpinned by some evidence of efficacy. It is very unlikely that every organisation would have the capacity to do so, so some 'ICO verified truths/principles' could be valuable for everyone.

We strongly recommend that the Commissioner makes use of these paragraphs in Clause 123[12] on transition, that offer the ICO a possible 12 months breathing room, to not rush into these more complex and controversial aspects of the proposed Code (Group B), beyond data protection and GDPR (Group A), i.e.:

> *(5) A code under this section may include transitional provision or savings.*
>
> *(6) Any transitional provision included in the first code under this section must cease to have effect before the end of the period of 12 months beginning when the code comes into force.*

Part of the Code which lies within the ICO current area of expertise could be put in place soon, and assess what changes are seen, the effects on capacity and enforcement can be measured and delivered, and unintended consequences mitigated for the second revision.

A twelve-month trial period before Group B changes, could give the opportunity for both a trial sample population of ISS to be tested, and the effects on data subjects (children) to be assessed, changes identified over time, and the consequences of the Code to be assessed -- as well as its untested effects on capacity and capability of the ICO for the implied changes, expected as a result of the features of both Group A and B.

A second phase of the Code implementation,-- which could include expansion or fixes to flaws found in the implementation, could begin once more work has been completed on Online Harms, beginning in twelve months after the initial, limited adoption, to ensure:

- avoidance of duplication of effort,
- a manageable approach, and a

[11] The LEGO ICO stage one consultation response https://ico.org.uk/media/about-the-ico/consultation-responses/2018/age-appropriate-design-code-responses/2260152/lego.pdf

[12] The basis for this Code, Clause 123, UK Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/section/123/enacted

- joined-up synchronised time period for government and industry to address appropriate standards which could be agreed and enforced.

We suggest the Code application might be applied to a sample population within schools in England and Scotland for the first twelve months which would offer a population of children in which age gating via AV would not be necessary, and could also enable oversight of the tools and ISS trialled 'in the wild', before and after Code implementation. This could also create case studies for learning and the benefit of other industry and innovators, and -- should it create harms; would limit that to a potentially known user group.

The ethical implications of such a trial may need considered as part of a research ethics committee -- however, since the alternative is rolling out this new Code in effect, untested, on the whole population, its ethical assessment is likely better in the trial group than outside it.

We further recommend that the ICO schedules and publishes dates for a rolling review period, and a date for proposed modifications once in place, that Clause 123(2) permits.

Timing and Risk of Overreach into Online Harms

We urge the Commissioner to focus attention in the Code drafting, only, but at the very minimum for the first 12 months, narrowly on children's personal *data processing*, (Group A) and playing an effective role in that remit, not overreach into broad online harms.

We note the heavy skew in balance of Stage One responses is about online harms, and accept that input may shape the Code, but it should not try to do something beyond its statutory and regulatory remit no matter how loud the calls to do so. We recognise and welcome the wide discussion of young people's experiences online, and note the view of young people themselves from evidence from youth juries, in the 5Rights collaborative UnBias and Csma projects by the Horizon Digital Economy Research Institute at the University of Nottingham[13] around persuasive design. As well as evidence on take down and abusive social media posts submitted by the BCS[14] and duty of care by the Carnegie Trust[15] which makes passing comment on AV. However, much of this debate is outwith the scope of data protection, or its effective regulation by the ICO. There is a common generalised conflation of concerns around content sharing beyond trusted friends (design of front end user settings), and limited understanding of the implications or effects for data processing by companies (design for back end data privacy and processing).[16]

These topics are under parallel consideration in the DCMS consultation White Paper, and are risks for which the staff at the ICO are unqualified to assess and unqualified to therefore effectively enforce in any DPIA (as we term, what falls under the Group B) in areas of the Code that it seeks to address in addition to privacy and data protection issues in (15):

> *"DPIAS. Step 5: Identify and Assess Risk*

[13] Horizon Digital Economy Research Institute at the University of Nottingham ICO AACOP stage one consultation https://ico.org.uk/media/about-the-ico/consultation-responses/2018/age-appropriate-design-code-responses/2260169/horizon-digital-economy-research-insitute-university-of-nottingham.pdf

[14] BCS ICO AACOP stage one consultation https://ico.org.uk/media/about-the-ico/consultation-responses/2018/age-appropriate-design-code-responses/2260199/bcs.pdf

[15] Carnegie Trust ICO AACOP stage one consultation "The NSPCC persuaded us that a duty of care could be applied to all social media, not only the largest." https://ico.org.uk/media/about-the-ico/consultation-responses/2018/age-appropriate-design-code-responses/2260317/carnegie-uk-trust.pdf

[16] Diana Award ICO AACOP stage one consultation https://ico.org.uk/media/about-the-ico/consultation-responses/2018/age-appropriate-design-code-responses/2260181/the-diana-award.pdf

- *Physical harm*
- *Online grooming and sexual exploitation*
- *Anxiety, self-esteem, bullying*
- *Access to inappropriate content*
- *Misinformation or restriction of access to information*
- *Encouraging excessive risk taking or unhealthy behaviour*
- *Undermining parental authority*
- *Compulsive use or attention deficit disorders*
- *Excessive screen time(*)*[17]
- *Interrupted or inadequate sleep patterns*
- *Unfair commercial pressure (where unrelated to data collection)*
- *Other broad disadvantages."*

The protection of natural persons in relation to the processing of personal data is a fundamental right and it would be foolish if in overstepping the scope of legislation intended to support that right, more harm is caused to that right by the ICO regulation than reduced, through the Code's inevitable effects of rushed implementation for children's privacy.

The well intended aim behind the Code is to better protect children and their use in particular of online services that are proponents of 'move fast and break things'. It would be a grave mistake to adopt the same model in this Code through impatience and over-ambition.

Pursuing an overly broad scope of content which the legislation simply does not demand and which does not sit within the ICO capability to support -- without first doing due diligence of its delivery impact on children and industry, is reckless from both a moral and practical perspective.

Where the Code strays from its remit of Data Protection law, and Clause 123 of the Data Protection Act 2018, there are significant practical and reputational risks for the ICO as well as to the children the Code aims to better protect:

- Lack of enforcement to date, while often blamed on lack of ICO capacity, will not be improved by adding new duties to staff to understand data processors' behavioural design, standards or delivery, which is far outside the remit of data protection
- Overreach in scope of content or geography will mean failure to enforce
- Expectations will not be met, and carries reputational risk for the ICO and Ministers.
- Industry may design out of fear, not good intent, and an over cautious approach will shift the risks of penalty from processors, onto children's privacy. There is no clear, strong, and effective mitigation of this significant risk created by parts of the Code.
- Duplication of ad-hoc efforts will create confusion and mixed messages in the press and from processors moving towards moving goals. This will not help children, or parents, to have clearer understanding of their rights, nor better protections.
- Increased data collection through confusion that AV is a necessity, also likely results in weak security open to breaches while standards are neither open, interoperable or understood.

[17] There is no evidence that this should be considered a risk as opposed to preference of opinion, and this should be removed: UK Chief Medical Officers' (CMO) commentary on 'Screen-based activities and children and young people's mental health and psychosocial well-being: a systematic map of reviews'.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777026/UK_CMO_commentary_on_screentime_and_social_media_map_of_reviews.pdf

Territorial scope

Territorial scope appears unclear, and unmanageable. While “relevant information society services” means information society services which involve the processing of personal data to which the GDPR applies, there is a real risk that the good players will be unduly penalised, and bad actors will simply ensure they have no establishment in the UK. The ICO does not enforce today on Australian, US, China or Russia based education apps collecting and in some cases publishing school children’s personal data online. We do not need a new Code in order to enforce the basic principles of Data Protection law but they are simply unenforceable. It seems foolish rather than ambitious to create something further that is unenforceable by-design, that undermines the legitimacy and seriousness of the Code aims. Our position on this from the *ICO stage one consultation (*para 23) remain as they were.[18]

Over focus on some children/services at the expense of others

We also urge the Commissioner in paying such significant attention to a subset of the private sector of children’s data processing, not to neglect monitoring and enforcement of the public sector, with particular regard to apps in education and health in the public sector that:

- Enable data processing, which reduces respect for rights to privacy and family life
- Embed a false notion of a universal ‘digital age of consent’ at age thirteen.

Data protection in practice can undermine privacy

Lack of respect for the human rights law right to privacy and family life, and Article 16 in the UNCRC are, becoming perhaps surprisingly embedded in developing UK data protection laws which prioritise free flow and the management of data, above privacy.

There is little consideration given in this Code, how the application of each area will work in practice where the legal basis for processing deviates from consent 6(a), and where it rarely applies, for example processing data from ISS via the UK state education sector.

For Annex B: Lawful basis for processing: We note broad children’s data processing in education is not included in the published ICO regulatory strategy workstream 2017-21, but it does include a focus on children’s privacy. But as an example how little this is respected in schools today, or by companies in schools, the law on consent requirements for biometric data processing in UK schools (Protection of Freedoms Act 2012)[19] that may fall into scope with regards to ISS (screen capture of behaviour and movement) preceded this explicitly in UK data protection law before 2018, but it is very often overlooked by schools, and applied in ways that make it hard to refuse. This is the same for processing Google Classroom which divides its services into Core and Additional services, and suggests in its privacy policies that schools must obtain consent for processing personal data from its Additional Services -- ignoring the fact that this basis can rarely apply to everyday routine data processing in schools, as there is either no choice at all offered to children and parents, or it is impossible to exercise freely given the power imbalance of parent-child-school.

[18] Defenddigitalme response to ICO stage one consultation (para 23) https://defenddigitalme.com/wp-content/uploads/2018/09/defenddigitalme_AACOP_ICO_FINALV1.1.pdf

[19] Protection of Freedoms Act 2012 Part 2, para 26. http://www.legislation.gov.uk/ukpga/2012/9/part/1/chapter/2/enacted

More detailed areas for consideration

Age groupings, and their description

The Code basis in the UK Data Protection Act 2018 (Clause 123) does not require age brackets, only that the Commissioner has "*regard to the fact that children have different needs at different ages.*" Annex A suggests these are set, but without broad support.

We note many of the various input to the *ICO stage one consultation* in Autumn 2018 like us, have suggested hard age brackets rather than capacity are flawed. This included Google[20], but urge that their use of the terminology is not language used by the ICO or its staff, as we have heard since the last stage of consultation. Thirteen is not a UK "digital age of consent".

We ask that wording in the Code on age, and external ICO communication on the subject, should be very clear not to accept common commercial company or media language, and try to avoid its use becoming embedded in everyday discussion of children's data processing.

Current wording says, "*13 is the age at which children in the UK are able to provide their own consent to processing*." It would be significantly better to indicate that, "*13 is the age at which the Data Protection Act 2018 permits data from children in the UK to be processed using their own consent as a lawful basis for the processing."*

Consent requires an informed individual with the capacity for understanding, and an implied grasp of reasonable expectations and the foreseeable consequences of processing, none of which is captured by this false phrase, "a digital age of consent."

We agree with Internet Matters[21] comment in their response to the *ICO stage one consultation* that the merits of breaking down below age 8 would seem to be unnecessary.

However, it is our opinion that some of their own partners do not follow good practice in school children's data processing today, including processing sensitive special data category data in the US, and some of whose current practices may not meet current UK Data Protection law or have proven past track records of poor ethical practice[22], or data security[23] for children. We therefore caution against over reliance on the imbalanced weight of the number of commercial consultation responses at any stage of this Consultation.


Founding Members: **BT, Sky, TalkTalk & Virgin Media**
Members: **BBC & Google, EE, PlusNet, Now TV**
Corporate Partners: **Huawei, Facebook, Instragram**
Supporters: **Twitter, Dixons Carphone, Nokia, Kurio, Smoothwall & KCom**

All these organisations have contributed both financially and in-kind to Internet Matters and we are continuing to make progress in securing new Partners & Supporters. In the past we also have undertaken projects with Disney, Halifax, Barclays, Impero and McAfee.

[20] Google Response to Stage One
https://ico.org.uk/media/about-the-ico/consultation-responses/2018/age-appropriate-design-code-responses/2260166/google.pdf
[21] Internet Matters ICO stage one consultation response
https://ico.org.uk/media/about-the-ico/consultation-responses/2018/age-appropriate-design-code-responses/2260171/internet-matters.pdf
[22] Facebook pays teens to install VPN that spies on them (2019) https://techcrunch.com/2019/01/29/facebook-project-atlas/
[23] Security flaw found in school internet monitoring software
(2015) https://www.theguardian.com/technology/2015/jul/14/security-flaw-found-in-school-internet-monitoring-software

The Statutory Foundations for Support of Age Verification

There is no requirement in Clause 123 and its legal footing, for the extensive age verification processes which this version of the Code suggests should now, not only apply to services targeted at children but that much more vaguely, likelihood of being accessed by a child, that has moved in scope to seem to mean, *'in any event of its use by a child*' without proportionate measure of balance of risk, even if a minority of children were to use a low risk service. Proposals (p13) now appear to suggest the aim is to age-gate every ISS user.

There appears to be no attention being paid to the context of Article 8(2) *"Conditions applicable to child's consent in relation to information society services,"* within the broader GDPR and requirements of Recital 57 and Article 11.

> *(57) If the personal data processed by a controller do not permit the controller to identify a natural person,* ***the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.*** *However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanisms such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.* [24]

Age Verification and Parental Consent

It is technically possible to age verify in ways that are safer and more effective than others. The positioning and balance of how AV is set out in the Code proposals gives the intended or unintended message, that robust age verification is a required measure. To promote doing so, and suggesting it must happen with urgency will have harmful unintended consequences. The untested application of age verification at scale, may have lifetime and population-wide effects as a result of the collection of hard identifiers and normalisation behaviour in children and young people.

Parental consent in principle can be problematic for children's exercise of their own rights.

- Participation can be limited by parents who withhold consent
- Age verification norms currently focus on payment methods only available to over 18s, such as credit cards. Use of this disadvantages those families who have none; for example Google Family Link, that uses a credit card and 30 cent charge.
- The Code should set out what happens to transition children out of the scope of the Code of Practice application at age 13 and at age 18. The current lack of attention to this poses children a grave risk of being set up for more "lawful" exploitation from 13.

There has been little attention given to the practical implications for data processors, when parental consent expires for an older child, or a child as they transition to an adult at 18, where consent was collected as basis for the processing of the personal data about a child.

[24] GDPR https://defenddigitalme.com/wp-content/uploads/2019/06/CELEX_32016R0679_EN_TXT.pdf

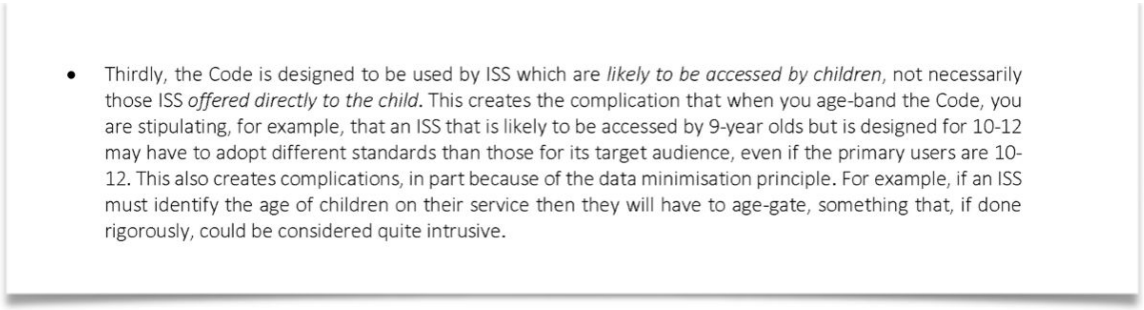
If AV requirements become embedded in a statutory Code, it will likely favour the existing 'tech giants' that rely on social log-ins across multiple platforms and apps, enabling them to become the de facto keeps of age gates across the Internet and normalise a reduction in privacy (such as Google log-in for their own apps, third-party apps, news, YouTube etc).

Right now, Google Family Link, emails every COPPA-protected US thirteen year old with an account on their birthday, to suggest the removal of parental controls, and therefore has a massive reach into a pre-packaged set of users to migrate to more invasive uses of personal data including linkage across all services, without oversight, from age thirteen, with unmanageable privacy policies[25] -- risks to privacy[26] which not every child may have been subjected, without enforced age-gating and is unlikely to understand in any case.

> *"When your child turns 13 (or the relevant age as determined by applicable law in your jurisdiction), they are eligible to manage their account on their own. If your child chooses to manage their Google Account, you will no longer have access to, or be able to exercise control over their account, unless you and your child later choose to set up supervision again through Family Link. Before your child becomes eligible to manage their own Google Account, we will notify you and your child."*[27]

While it may be obvious to the data protection community, it may not be as obvious to processors, that the shift from child to adult should not automatically mean that a processor can cease to apply the Code and also continue to use the personal data collected under it.

The LEGO company contribution to the stage one consultation also said that age gating goes directly against the data protection principle of data minimisation, and would be intrusive:



- Thirdly, the Code is designed to be used by ISS which are *likely to be accessed by children*, not necessarily those ISS *offered directly to the child*. This creates the complication that when you age-band the Code, you are stipulating, for example, that an ISS that is likely to be accessed by 9-year olds but is designed for 10-12 may have to adopt different standards than those for its target audience, even if the primary users are 10-12. This also creates complications, in part because of the data minimisation principle. For example, if an ISS must identify the age of children on their service then they will have to age-gate, something that, if done rigorously, could be considered quite intrusive.

Current suggestions for 'robust' measures to age-gate all users are reckless to have up front without safeguards, and are not ready to implement in a Code without any care for its effects. This requires further work, and positioning of AV related priorities.

We believe that mitigating requirements at minimum might include a duty to:

1. Make clear that 'robust' age verification should still apply principles of data minimisation and cannot process ID data collected for any other purpose, at any time.

2. The suggestions of 'show me' style tools, and data usage reports, as proposed by 5Rights to enable consistent ways in which a child could expect to understand what their digital footprint looks like and where it has gone.

3. A delete-and-re-collect-if-approved-model at both age 13 and 18, might well apply to

[25] Google Family Link privacy policies https://families.google.com/familylink/privacy/notice/
[26] Blog: Google Family Link for under 13s, privacy friend or foe? (March 2017) https://jenpersson.com/google-family-link/
[27] Google Family Link https://families.google.com/familylink/

a) consent, and
b) any personal data, including pseudonymous data processing (often, for example, still not considered as personal data by many school processors).

4. Encryption, authentication, anonymity in communication, and privacy by design.

Age Verification has been insufficiently addressed to be safe

We cannot support the current ICO proposals for Age Verification as set out. Insufficient attention has been given to the risks and benefits for children, which the ICO itself addressed far better in its submission to the House of Lords Consultation on *Children and the Internet* in 2016, and we set out in more detail below.

The emphasis on age verification in the Code as set out, will be read as a demand for a disclosure of a greater amount of identifying data to the processor, than Article 8(2) requires, since Article 8 is strictly applied to ***children***, and on the basis of consent. That would be a grave mistake, and be very likely to cause more harm than it tries to reduce.

> *"Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology."*

The ICO itself recognised this problem in its own response to the ICO House of Lords Consultation on Children and the Internet in September 2016, under three years ago[28]; after the adoption of the Regulation in the preceding April and under the same incumbent of the Office, when the ICO view of this in the GDPR was:

> *"**sceptical about seeing an approach that seeks to differentiate between children's and adults' sites as being in itself a solution to the problem of children's online protection,"***

and that:

> *"GDPR contains several provisions aimed at the protection of children's data. Essentially the GDPR seeks to introduce an age-based approach to protection, meaning that a child cannot consent to use an 'information age service' offered directly to him or her; there must be consent from the holder of parental responsibility. Although the wording is not entirely clear, **we take this provision as applying to commercial internet services specifically targeted at children. If such an approach is adopted in UK law, we think it could be difficult to apply in practice."***

Many of the very practical and remainder of the 2016 ICO recommendations on age appropriate specifications[29] are included in the Code, for example on transparency, and education, however there is suddenly a significant shift of position from the 2016 recommendations on Age Verification to those now, and we set out these parts here

[28] ICO House of Lords Consultation on Children and the internet in September 2016 https://defenddigitalme.com/wp-content/uploads/2019/06/house-of-lords-children-and-the-internet-ico-response-20160901.pdf
[29] All highlighted extracts ICO House of Lords Consultation on Children and the internet in September 2016 https://defenddigitalme.com/wp-content/uploads/2019/06/house-of-lords-children-and-the-internet-ico-response-20160901.pdf

highlighted in full, which includes that an appropriate approach to risk, would not always require age verification:

> mental competence of the prospective purchaser is not an issue. However, on balance we favour an approach where even quite young children can access appropriate online services without the consent of a parent or guardian, provided organisations have taken other safeguards. In our view a child should be able to take part in an online activity that presents little or no privacy risk and is of such a nature that the child in question is capable of understanding the implications for him or her. A good example might be accessing a pop-star's website and subscribing to a newsletter. (Of course children must be able to access confidential counselling services such as Childline without parental involvement.)

Extract from ICO House of Lords Consultation on Children and the Internet in September 2016.

These new 2019 Code proposals by contrast in (2) Age Appropriate Application, say (p22), "if your service is likely to be accessed by children but you don't know which users are children, you must apply the code to all users."

2. Age-appropriate application

> Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish children from adults.

That creates unnecessary risk, whilst potentially mitigating none. It goes on to suggest "Tailor the measures in this code to the age range of your users" but should tailor to risk.

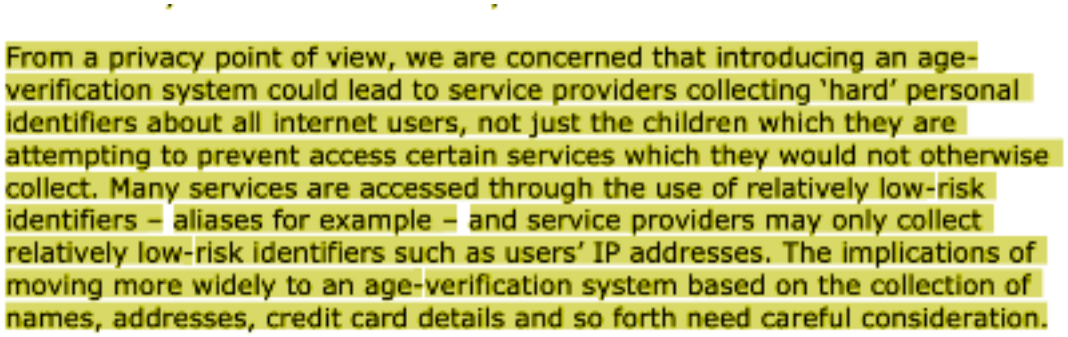
It is inevitable that statements such as the headline introduction on this topic (2), which do not mention proportionate risk requirements, or any context of what is necessary in law around data minimisation, and Recital 57, will lead to processors rushing to over compensate by reading this over simplified position without any other understanding of data protection law, as a duty to, "have robust age verification mechanisms to distinguish children from adults."

This will harm children's privacy and reduce their data protections in practice, and with it, that of adult populations present and future. It is inadequate to legislate on this with lay understanding of the technology and its implications.

If the ICO has engaged on 'robust' Age Verification with a variety of industry standard bodies, including the W3C and IEEE, this new Age Appropriate Code of Practice proposal fails to publish recommendations on what might be the global standards it seeks to measure ISS providers against. How 'robust' is enough? Mitigating risk is a vague notion that will inevitably lead to increasingly punitive and restrictive data processing measures.

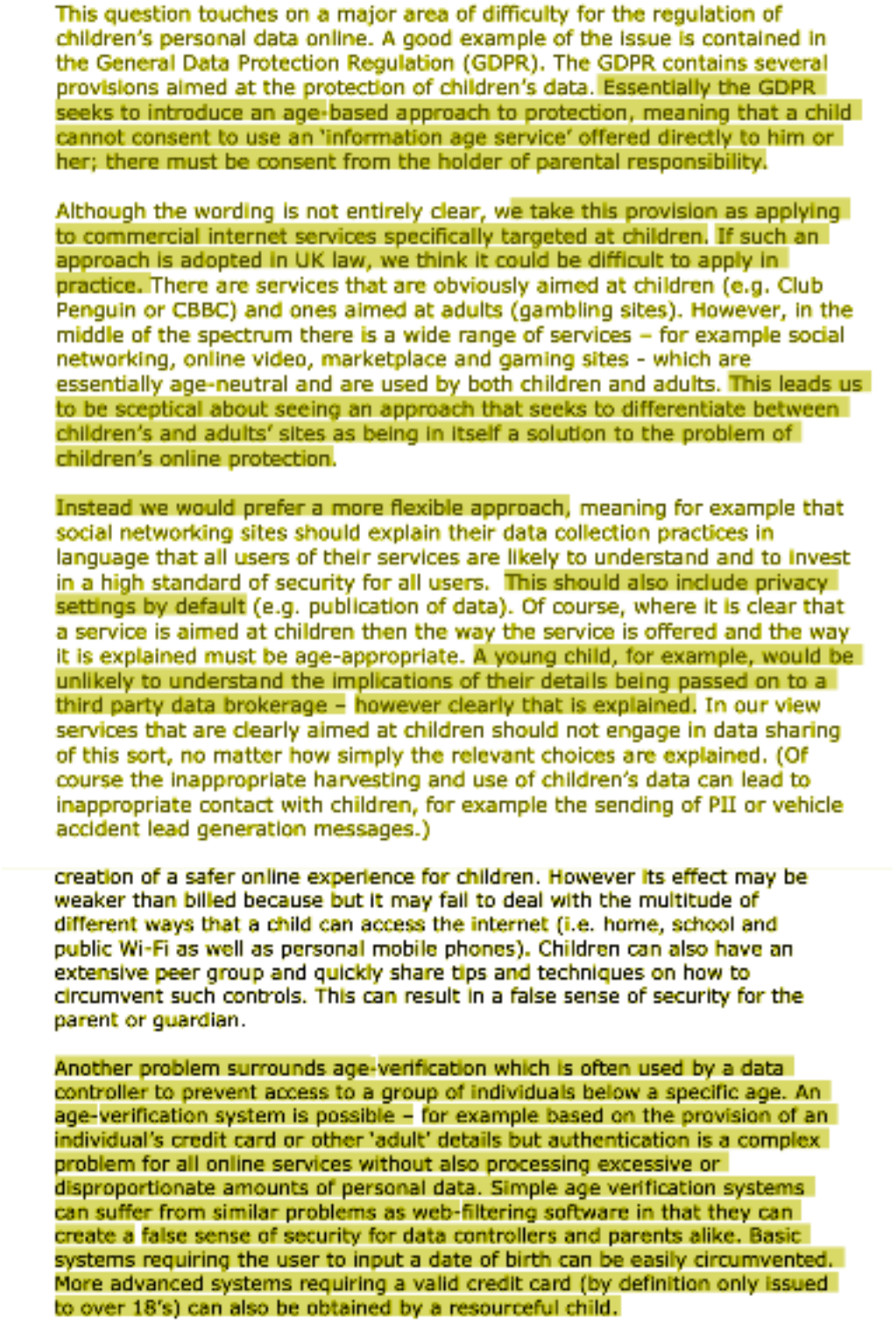
As we also set out in our September 2018 *ICO stage one consultation submission*, safer, *"Age Verification (AV) must verify the single attribute of age, not capture date-of-birth, or more personal data. Re GDPR recital 64 on Identity Verification, "A controller should not retain personal data for the sole purpose of being able to react to potential requests,"* so too did the ICO 2016 recommendations on *Children and the Internet* recognised that the collection of 'hard' personal identifiers posts a risk of all Internet users, and children, that they would not otherwise collect. Recital 57 in the GDPR in effect prohibits this, and suggests instead that *"Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller,"* these do not need an everyday identity.

The ICO 2016 recommendations on Children and the Internet are very different from the suggested requirements of the Code, and do not appear to have had thorough or '*careful consideration*' that the ICO in September 2016 found would be necessary :



From a privacy point of view, we are concerned that introducing an age-verification system could lead to service providers collecting 'hard' personal identifiers about all internet users, not just the children which they are attempting to prevent access certain services which they would not otherwise collect. Many services are accessed through the use of relatively low-risk identifiers – aliases for example – and service providers may only collect relatively low-risk identifiers such as users' IP addresses. The implications of moving more widely to an age-verification system based on the collection of names, addresses, credit card details and so forth need careful consideration.

Extract from ICO House of Lords Consultation on Children and the Internet in September 2016.



This question touches on a major area of difficulty for the regulation of children's personal data online. A good example of the issue is contained in the General Data Protection Regulation (GDPR). The GDPR contains several provisions aimed at the protection of children's data. Essentially the GDPR seeks to introduce an age-based approach to protection, meaning that a child cannot consent to use an 'information age service' offered directly to him or her; there must be consent from the holder of parental responsibility.

Although the wording is not entirely clear, we take this provision as applying to commercial internet services specifically targeted at children. If such an approach is adopted in UK law, we think it could be difficult to apply in practice. There are services that are obviously aimed at children (e.g. Club Penguin or CBBC) and ones aimed at adults (gambling sites). However, in the middle of the spectrum there is a wide range of services – for example social networking, online video, marketplace and gaming sites - which are essentially age-neutral and are used by both children and adults. This leads us to be sceptical about seeing an approach that seeks to differentiate between children's and adults' sites as being in itself a solution to the problem of children's online protection.

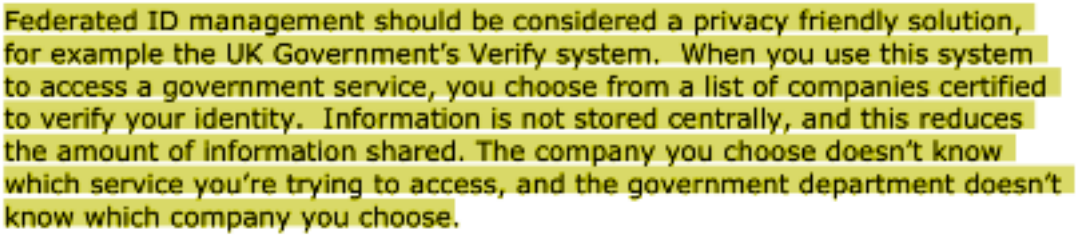
Instead we would prefer a more flexible approach, meaning for example that social networking sites should explain their data collection practices in language that all users of their services are likely to understand and to invest in a high standard of security for all users. This should also include privacy settings by default (e.g. publication of data). Of course, where it is clear that a service is aimed at children then the way the service is offered and the way it is explained must be age-appropriate. A young child, for example, would be unlikely to understand the implications of their details being passed on to a third party data brokerage – however clearly that is explained. In our view services that are clearly aimed at children should not engage in data sharing of this sort, no matter how simply the relevant choices are explained. (Of course the inappropriate harvesting and use of children's data can lead to inappropriate contact with children, for example the sending of PII or vehicle accident lead generation messages.)

creation of a safer online experience for children. However its effect may be weaker than billed because but it may fail to deal with the multitude of different ways that a child can access the internet (i.e. home, school and public Wi-Fi as well as personal mobile phones). Children can also have an extensive peer group and quickly share tips and techniques on how to circumvent such controls. This can result in a false sense of security for the parent or guardian.

Another problem surrounds age-verification which is often used by a data controller to prevent access to a group of individuals below a specific age. An age-verification system is possible – for example based on the provision of an individual's credit card or other 'adult' details but authentication is a complex problem for all online services without also processing excessive or disproportionate amounts of personal data. Simple age verification systems can suffer from similar problems as web-filtering software in that they can create a false sense of security for data controllers and parents alike. Basic systems requiring the user to input a date of birth can be easily circumvented. More advanced systems requiring a valid credit card (by definition only issued to over 18's) can also be obtained by a resourceful child.

Extract from ICO House of Lords Consultation on Children and the Internet in September 2016.

Federated ID management is not even mentioned in these new 2019 proposals, and appears to propose moves away from child data protection and privacy, towards a higher risk, less secure, and potentially lazy option for processors, against a child's best interest.



Extract from ICO House of Lords Consultation on Children and the Internet in September 2016.

As defenddigitalme set out in our response to the 2018 *ICO stage one consultation* (para 227), *"Anonymous personas must also be possible for children of any age to maintain online."*

Public interest

There is lack of clarity on Public Task and Consent, and therefore where ISS may fall under the remit of the Code. Baroness Ludford was one of many peers to point out difficulties in the House of Lords during the passage of the UK Data Protection Bill, on October 10, 2017[30]

> *"We may need seriously to look at the lack of definition of "substantial public interest" as a basis for processing sensitive data, or even of public interest….There is also concern that the safeguards for profiling and other forms of automated decision -making in the Bill are not strong enough to reflect the provisions of Article 22 of the GDPR. There is no mention of "similar effects" to a legal decision, which is the wording in the regulation, or of remedies such as the right of complaint or judicial redress."*

This is still unclear where it applies to a child, and will come into conflict with apps in the public sector which fall under the Code, but cannot reasonably process on a consent basis.

Commercial products are widespread in schools and higher education bodies are increasingly buying AI solutions, sold as ways of reducing workload and increasing efficiency through reduced admin. time. The resulting rapid transfers of pupil data to commercial third parties, have no oversight. If processing should not routinely concern a child, there will need to be significant change of practice, and very strong oversight and enforcement in England, to respect the intent of the GDPR, this WP29 guidance, and CoE Principle 3.5,[31] "*profiling of persons who cannot freely express their consent be forbidden, especially, for example, adults with incapacity and children, within the meaning of the UNCRC.*"

Design standards

Open standards and development communities need to be involved to collaborate on the scope and feasibility GDPR requirements, and in particular Article 8(2) and Group B impacts.

[30] http://hansard.parliament.uk/Lords/2017-10-10/debates/22188EC1-6BAB-4F06-BE64-5831ABAF78E2/DataProtectionBill(HL)
[31] CM/Rec (2010)13 adopted by the Committee of Ministers on 23 November 2010

Ability to seek redress under the Code

Right to Representation Article 80(2)

We would welcome if the ICO would again address with government the need for a clear route of redress for children, so that this Code may be of any practical use. There is too little attention paid to this aspect of the Code. If existing Data Protection law were followed in full, and with appropriate levels of enforcement, the perceived need for this Code would be reduced. What practical difference the Code makes to children's ability to enact their rights and how, needs seriously addressed.

During the passage of the UK Data Protection Bill, in Committee on November 22, [col 225] Baroness Kidron spoke of children and their right to representation saying children need to have an informed advocate if they have a complaint. *"the amendment usefully aligns with the recommendation made by the Children's Commissioner and the House of Lords Communications Committee that children urgently need champions in the digital environment."*

Lord Stevenson[32] mentioned children specifically in his call to restore GDPR Article 80(2).

As the Children's Society wrote in their briefing[33], we cannot expect children to have to trawl the Information Commissioner's Office website to learn about their rights– they should be proactively and regularly communicated to children, in a way which is easy for them to understand.

Their right to be heard and participate in decisions affecting them, both as individuals and as a group has been absent in shaping GDPR. Article 12 of the UN Convention of the Rights of the Child support the intention of GDPR

1) *Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.*
2) *For this purpose, the child shall in particular be provided the opportunity to be heard in any judicial and administrative proceedings affecting the child, either directly, or through a representative or an appropriate body, in a manner consistent with the procedural rules of national law.*

It is therefore incumbent on those responsible for children and their data management to proactively ensure child rights and needs are championed. GDPR makes clear the responsibilities of data controllers and processors exist as part of a relationship and power balance, between duties in practical tasks, and mitigating the risks to the rights and freedoms of individuals whose personal data are entrusted in care.

[32] Hansard Data Protection Bill (House of Lords) November 22, 2017 (Col 227)
https://hansard.parliament.uk/lords/2017-11-22/debates/0DD49E5D-F04B-4ACA-A8CF-7BC6FB4D549B/Debate
[33] https://www.childrenssociety.org.uk/sites/default/files/amendment-20-education-on-rights-of-data-subjects.pdf

Baroness Lane Fox pointed out at Second Reading on October 10, (**Col 156)**
"that we are sleepwalking into a dystopian future if we do not work hard to simplify the Bill and make it accessible to more people, the people to whom I feel sure the Government must want to give power in this updated legislation."

If the government were serious about empowering children to enact their rights, as it appears to support in this Code, why has the right of civil groups to take action on behalf of individuals been actively removed from the UK context for the GDPR? As she pointed out,

*"Instead, **the Bill places a huge onus on individuals, who may lack the know-how and the ability to fight for their rights**. As has been mentioned, article 80(1) of the GDPR allows for representative bodies—for example, consumer groups—to bring complaints at the initiation of data subjects. **Article 80(2)** allows those groups to bring complaints where they see infringements of data rights without an individual having to bring the case themselves."*

Recital 27

The Code only covers the living. Recital 27 allows for Member States to provide for rules regarding the processing of personal data of deceased persons and we would like some future consideration and amendments to the Code to consult on this for children, particularly with the sensitive nature of cases and unknown future uses of personal data which may have implications for other family members.

ICO governance of the Code

The ICO will need a method of identifying processors that fall under the scope of the Code. An addition to the Data Protection Public Register of Fee Payers, may enable such processing to be acknowledged. We also suggest that adding special category data as a separate sub-set, for the processing of children's personal data, in particular biometric data.

We suggest future review dates are scheduled and published in advance, under the Clause 123 paragraphs (2), (5) and (6) as set out above. This will bolster the legitimacy of the ICO process and its public interest obligations to listen to developing industry standards, as well as all other stakeholders in (4) (a-e) who may want to and be eligible to join this process later, as technology changes, and the risks and benefits become apparent.

The ICO should plan now, in order to avoid that unintended consequences cannot be reviewed simply due to other ICO priorities and capacity in its future workstreams.

Supporting References

Our response to the ICO Statutory Age Appropriate Code of Practice (Data Protection Act 2018) *stage one consultation*[34].

[34] Defenddigitalme Stage One consultation reponse
https://defenddigitalme.com/wp-content/uploads/2018/09/defenddigitalme_AACOP_ICO_FINALV1.1.pdf

Working Party 29 Guidelines on Automated individual Decision-making and Profiling[35] *for purposes of Regulation 2016/679.*

2017 International Working Group on Data Protection in Telecommunications- Working Paper on e-Learning Platforms | "*Legislation covering educational institutions may not adequately address new technological trends in learning processes and the extended scope and purposes of data processing in the context of e-learning and learning analytics*." [36]

UK Chief Medical Officers' (CMO) commentary on '*Screen-based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews'.*

The UK Data Protection Act Clause 123

123 Age-appropriate design code

(1) The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children.

(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and such other persons as the Commissioner considers appropriate, including—

(a) children,

(b) parents,

(c) persons who appear to the Commissioner to represent the interests of children,

(d) child development experts, and

(e) trade associations.

(4) In preparing a code or amendments under this section, the Commissioner must have regard—

(a) to the fact that children have different needs at different ages, and

(b) to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child.

(5) A code under this section may include transitional provision or savings.

(6) Any transitional provision included in the first code under this section must cease to have effect before the end of the period of 12 months beginning when the code comes into force.

(7) In this section—

"age-appropriate design" means the design of services so that they are appropriate for use by, and meet the development needs of, children;

"information society services" has the same meaning as in the GDPR, but does not include preventive or counselling services;

"relevant information society services" means information society services which involve the processing of personal data to which the GDPR applies;

"standards of age-appropriate design of relevant information society services" means such standards of age-appropriate design of such services as appear to the Commissioner to be desirable having regard to the best interests of children;

"trade association" includes a body representing controllers or processors;

"the United Nations Convention on the Rights of the Child" means the Convention on the Rights of the Child adopted by the General Assembly of the United Nations on 20 November 1989 (including any Protocols to that Convention which are in force in relation to the United Kingdom), subject to any reservations, objections or interpretative declarations by the United Kingdom for the time being in force.

[35] Working Party 29 Guidelines on Automated individual Decision-making and Profiling https://defenddigitalme.com/wp-content/uploads/2017/12/20171025_wp251_enpdf.pdf

[36] https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2017/25042017_en_2.pdf