ICO's Age Appropriate Design Code – Taylor Wessing LLP Consultation Response

We welcome the opportunity to provide a response to the ICO's consultation on the Age Appropriate Design Code (the "code"). As an international law firm with a large presence in the technology and digital sectors, Taylor Wessing LLP has many clients who, whilst supportive of the objective of creating safe online environment for children will be impacted by the code, particularly if it is approved by Parliament and adopted by the ICO in its current form.

A number of Taylor Wessing's clients have expressed significant concerns about the scope and terms of the code but have felt unable to make a submission on their own account and not had the option of feeding in views to an industry body response. Therefore, this submission reflects a summary of the themes raised by multiple clients rather than the views of Taylor Wessing LLP or those of any member of the Taylor Wessing Team. There is a strong view amongst those with which we have spoken that there should be further consultation on the code and in particular a more comprehensive assessment of the real needs of children as well as a full economic impact assessment to determine the likely financial cost of the code, if adopted in current form.

Because of the thematic nature of this submission it would not be appropriate or indeed possible to respond to the individual questions raised in the online response form provided by the ICO as the various clients that have expressed views to us have differing concerns. We trust that this submission will be acceptable in its current form. Any questions in relation to this submission should please be directed to Sally Annereau and/or Jo Joyce of the Taylor Wessing (UK) Data Privacy team.

SUMMARY – Taylor Wessing client responses

Defined terms / standards	▶ Code inconsistently refers to information society services (ISS) and 'relevant online services' and 'online services'. ▶ Code refers both to services 'likely to be accessed by children' and 'likely to be used by under 18's'. This is unclear, wide in scope, and not aligned with other established terms e.g. 'offering' services to data subjects', or directly offering to children (as in the GDPR's recitals).
Scope	▶ Age appropriate design is not just a data protection issue, yet other aspects of age appropriate design have been included in the ICO's draft code. Code refers to a range of non-data protection risks (e.g. online grooming, bullying, peer pressure, nudge techniques/'stickiness') which are more to do with internet safety and online harms generally. These may be more appropriately dealt with by other bodies (e.g. Children's Commissioner for England). ▶ Code references industry codes of practice & guidance (e.g. CAP guidelines, PEGI ratings) in such a way that it has the effect of giving statutory force to non-statutory codes.
Conflicts or points of clarity	▶ Potential conflict with the GDPR in terms of the age of a child (Code deems this to be up to 18). The GDPR does not define a child but rather the range of 13-16 is recognised in the GDPR as the age threshold at which parental consent may no longer be needed). ▶ Code refers to parents' involvement in decision-making for their children without recognising that responsibility often falls away at 16. ▶ Code fails to account for capacity/reason and sophistication of older teenagers (e.g. 16-18). ▶ Risk of inadvertently undermining UK compliance with aspects of the UN Convention on the Rights of the Child (e.g. rights of expression, association, and access to information from media).
New data protection risks	▶ Code seeks to effectively require all users to be treated as if children as a default or to require more complex and intrusive processing through age verification mechanisms. Age verification requirements may conflict with data minimisation obligations, and potentially create large pots of ID information which will be a target for cybercrime and fraud. ▶ There is a general lack of guidance for technical implementation.
UK industry impact + Brexit	▶ Code does not apply to organisations with no establishment in the UK and whose lead supervisory authority is not the ICO. The cost of complying may make some businesses consider moving out of the UK and may dissuade start-ups with a choice of establishment. ▶ Risk of divergence from the EU27, which may affect any future UK adequacy ruling.
Adequate consultation	▶ It is not apparent that the research commissioned by the ICO engaged with the views of children in any significant or extensive way in making its recommendations as to what content and tools may be appropriate at what age. The ICO is required to consult widely on the code (in particular, consulting children). The research underpinning the draft code appears not to have properly taken account of the views of children.

THEMES ARISING

1. Defined legal terms or standards

- The code appears to switch between referring to providers of information society services (ISS) and 'relevant online services' and 'online services' reflecting the fact that it does not attempt to define what is 'relevant' in any meaningful way, rather choosing instead to treat every ISS as relevant.

- The code refers both to services 'likely to be accessed by children' and 'likely to be used by under 18's. These terms are not directly the same. What is to be considered 'likely' will be obvious in some cases and hugely subjective in others. Further, the code is not aligned with existing legally established terms referred to in the GDPR, e.g. 'offering' services to data subjects.

- The code refers to detriment and damage interchangeably. These are different terms and can have different legal meanings.

2. Conflicting requirements or points clarity

- *Conflict/confusion with other UK laws*

  - The code refers to parents having a key role in deciding what is in the best interests of their children without recognising the fact that in many cases that responsibility can fall away after 16.

  - UK children below 18 are treated as being able to reason and act for themselves across a broad range of activities in the UK for which there are separate legislative provisions. The list is long but includes:

Age	Recognised responsibility
10	Criminal responsibility
13	Work (subject to hours limitations)
16	Finish education, Leave home, work, have sex, use contraception, seek confidential treatment from a GP, enlist in the army, get issued a standard passport, buy and care for their own pet, drive a motorised scooter on the public highway, register to vote.
17	Drive a car, buy/own an airgun

Section 123 of the DPA and its adoption without any nuance or interpretation in the code may create confusion and conflict, effectively creating online barriers to the exercise of certain legal rights that children already have.

  - Treating older teenagers (16+) as lacking capacity/reason in this regard, and establishing standards in relation to their online activities which do not reflect their level of sophistication. Some teenage internet users are extremely sophisticated – many 'white hat' hackers are under 18 and need little protection from online harms. This approach also risks artificially raising the level of complexity permitted for services targeting (often less digitally sophisticated) adults and vulnerable adults in particular.

- *Risks of creating divergence with the EU27*

  - The proposed code appears to create burdens additional to, the GDPR, moving so far beyond the GDPR that this seems likely to create as yet unforeseen difficulties, at a time when the government has explicitly stated its intention to remain aligned with the EU post-Brexit in respect of data privacy matters.

  - During the debates on the DP Bill, concerns were raised about the impact of the amendment regarding the scope of the Age-appropriate design code would go wider than the GDPR. Lord Ashton of Hide raised this in Committee (HL on 6.11.17) stating:

"I have to raise the issue of compliance with the GDPR, because we have a very real concern that these amendments are not compatible with it. The GDPR was designed as a regulation to ensure harmonisation of data protection laws across the EU. The nature of the internet and the transnational flow of data that it entails mean that effective regulations need international agreement. However

these amendments would create additional burdens for data controllers. Article 8 of the GDPR says that member states may provide by law for a lower age but it does not indicate that exercising this derogation should be conditional on other requirements. These amendments go further than permitted, creating a risk for our future trading relationships"

- *Risk of inadvertently undermining UK compliance with aspects of the UN Convention on the Rights of the Child (the "Convention")*

    - Article 13 of the Convention requires that children be free to express their thoughts and opinions and access all kinds of information – within the law.
    - Article 15 provides that children have a right to meet with other children and to join groups and organisations (which arguably, includes online freedom of association).
    - Article 17 provides that children have a right to access information from the media (though governments must take steps to protect children from harm).

    The code, as written, is broad and creates real risk and difficulty in achieving compliance for organisations meaning some may seek to restrict the access of children. Since the Government cannot force companies and organisations to provide digital services to children, care needs to be taken to ensure that measures do not have the effect of reducing the ability of children to access relevant digital services.

3. Guidance that creates data protection risks

- *Conflict with the GDPR*

    - There appears to be an inherent conflict between the role of the ICO in respect of the scope of its age appropriate design code obligations and that of the GDPR and the UK DPA18. The GDPR does not define a child although there is an implicit recognition within Article 8 that at age 16 parental responsibility will fall away, given from that age parental consent does not effectively have a role to play in providing lawful grounds for the processing of the data of a child.

    - Article 8.1 allows a member state to determine that the ability of a child to think for itself in the context of an information society service may be lower, a step the UK took by placing the threshold where, in effect, a child's own reasoning power must be replaced by that of the parent at below 13. It therefore appears wholly inconsistent with the aims and objectives of the GDPR and UK legislators to set wider standards capable of being interpreted against anyone up to the age of 18.

      As mentioned further below, it is not apparent that the specialist research conducted to inform the code, engaged with a significant number of children, in making its recommendations as to what content and tools may be appropriate at what age. The limits of the guidance should reflect those set by the GDPR.

- *Age verification*

    - The code recommends that a child appropriate service be provided to all and that adults step through age-verification to disable default child focused protections. This must be robust and effective, essentially requiring the collection of identity verification information in relation to all adults which conflicts directly with data minimisation obligations and potentially create large pots of ID information which will be a target for cybercrime and identity theft.

    - Those online services that wish to present the argument that they are not likely to be accessed by children must be able to prove this, again effectively requiring additional robust data on age verification and placing a heavy burden in the shape of an albeit rebuttable presumption upon site operators. The code after recommending this approach, emphasises the obligation to comply with data minimisation and storage and limitation and security obligations, without offering further guidance as to how these potentially contradictory obligations might be met.

- *Conflict with the intention of recital 38 of the GDPR*

Recital 38 of the GDPR is concerned with ensuring specific protections for children with respect to their personal data in connection with the "*collection of personal data with regard to children when using services **directly offered to** a child*" (emphasis added). This reflects far more active intent in targeting of services than

the broader scope of the intention of "likely to be accessed by children" within the approved amendment at section 123.

- *Conflict with the intention of Art 3 of the GDPR*

  Extra-territorial provisions are triggered in relation to **offering goods or services** by controllers outside the EEA (emphasis added). The focus of the GDPR here is that there must be an intention to offer. The code however places a further obligation on such sites given that even if they are not offering services to children but to others, they must also comply with the code if the site is likely to be accessed by children, going beyond the GDPR.

- *Relationship between the code, the economy and Brexit*

  - The ICO states the code does not apply to those whose lead authority for the purposes of the GDPR is other than the ICO and where they have no establishment in the UK.
  - The UK tech is expanding 2.6 times faster than the rest of the UK economy, according to Tech Nation's 2018 report. The digital tech sector is worth nearly £184 billion to the UK economy, up from £170 billion in 2016. For UK digital business, the cost of complying with the code may make some such businesses consider moving out of the UK and is likely to dissuade start-ups with a choice of establishment.
  - The code further says nothing about whether EU business will however be expected to comply with the Code in a post-Brexit scenario. To the extent the requirements are considered to go beyond and conflict with the GDPR this may seriously impact the ability of the UK to obtain an adequacy finding enabling the free flow of data (speaking to Lord Ashton's comment regarding the risk to our future trading relationships).

- *Default privacy settings and consent*

  The requirement for adults to prove their age in order to change default settings could be viewed as imposing consent as a lawful ground for processing where not relevant or appropriate or in collecting a double consent for certain processing, potentially conflicting with the UK implementation of PECR, such as where a service is able to rely on a soft opt-in for processing.

4. Guidance that could be achieved by other means

- The creation of a code with such broad scope and which allows for potentially constant change in the nature of the obligations it seeks to create, depending upon the pace of technological progress, risks the creation of significant moral hazard. The assertion that parents are likely to be unable to make appropriate decisions for their children in relation to online behaviour risks the development of a digital environment where parents rely upon reputable companies to protect their children, leaving them vulnerable to less scrupulous online actors. Responsible organisations have a crucial role to play but a responsibility should also rest with individuals and/or parents and carers (particularly in the case of children under 13 – the DPA 18's age of digital consent in respect of ISS).

5. Privacy, internet safety and online harms

- The code (section 4) requires services to not use personal data in ways that have been shown to be detrimental to children's wellbeing or that go against industry codes of practice and the ICO can take this into account in considering compliance with the age appropriate design code. This has the effect of giving statutory force to non-statutory codes by enabling for example, the ICO to enforce against a service if it does not properly consider the impact of the CAP code on content relating to fat or sugar content in foods or on other CAP code matters.

- The code speaks of the best interest of the child being a primary consideration but also focuses in detail on those aspects of the Convention that speak to the rights of parents rather than children. Recital 38 of the GDPR however focuses on the protecting the rights of children not those of parents.

- The code says that services should not process data in ways that have been 'formally established' as requiring further research or evidence to establish whether or not they are detrimental to the health or wellbeing of children. There is nothing to explain what 'formally established' means here and the code appears to effectively rule out processing in relation to activities that have not yet been established to be

detrimental. This appears to open the door to enforcement, based on mere hearsay or subjective views. The government has repeatedly spoken of the importance of evidence based policy – in this respect the draft code risks departing from that aim.

- The DPIA guidelines require services to consider a range of non-data protection risks associated with the service such as physical harm, online grooming, social anxiety, self-esteem, bullying, peer pressure, access to inappropriate content, nudge techniques/'stickiness' & misinformation.

6 Relationship between the code and Parliamentary intent

- *Relevant information society services **not** all information society services.*

  Section 123 (1) DPA18 refers to the ICO preparing a code of practice… on standards of age-appropriate design of **'relevant information society services'** (emphasis added) and not of all information society services. Many of the examples of harm and detriment given within Parliament as a reason for pointing to the need for the amendment initially focused on social media (with Facebook and Instagram and instant messaging being mentioned).

- *Lack of breakdown of what 'likely to be accessed by children' means*

  Section 123 (1) DPA 18 also refers to relevant information services 'likely to be accessed by children' and 'likely to be used by under 18's'. The code does not address in any detailed way whether services are likely to be accessed. The code simply distinguishes between sites aimed specifically at children and all other services who must prove why and how children are not likely to access their service. In practice this potentially places an obligation on every service to create age barriers that adults will have to step through.

- *Views of children*

  - The ICO must under Section 123 (3) consult widely on the code in particular capturing the voice of children. The ICO Commissioned research to inform the approach to the draft code, yet the approach to and results of that research reflected more the perceptions and attitudes of parents than those of children. The researchers openly acknowledge the limitations of their research in properly representing the viewpoint of the children whose interests the ICO is seeking to represent in particular:

    - the research reached out over 2000 parents but yet only engaged with 280 children,
    - an open online survey was completed by just 3 children.

  - In preparing the code the ICO is required to have regard to the UK's obligations under the UN convention on the rights of the Child. The convention also states that children have rights to personal freedoms and to participate in decision making. This means that they have a right to have their views listened to and to be taken seriously.

We would be happy where possible, to contribute to any further engagement or discussion on the responses to ICO's consultation, notwithstanding the time constraints imposed on the ICO to finalise the code by Parliament.