Supplementary document to Bird & Bird LLP's response to the ICO's consultation on the age-appropriate design code

This supplementary document provides further details on Bird & Bird LLP's response to the ICO's consultation on the age-appropriate design code. It addresses the following sections of the code:

1. Services covered by the code
2. Age verification mechanisms
3. Restrictions on data sharing
4. Profiling
5. Transparency
6. Data minimisation
7. Transitional period

1. Services covered by this code: a greater focus on UK children

The code follows the territorial scope of the DPA 2018. This means that it applies when personal data is processed in the context of the activities of an establishment of a controller or processor in the United Kingdom. The EDPB draft guidelines on the territorial scope of the GDPR suggest that if an organisation in the EU is taking decisions in relation to the processing of personal data carried out outside the EU, the GDPR would still apply to such processing (Examples 4 & 5 in the EDPB draft).

A number of our international clients with substantial UK operations explained that this would be relevant for them because their UK establishments take decisions (and are controllers) in respect of all personal data processed in connection with online services either worldwide, or outside of North America. These clients have already applied the GDPR in relation to such services. However, as noted below, the code imposes standards which are significantly more restrictive than those in the GDPR. Such clients expressed significant concern over the potential global reach of the code in this situation, which may result in their being subject to obligations which are inconsistent with legal obligations in other countries, or which affect the commercial viability of their services worldwide (rather than just in the UK).

Organisations with multiple establishments in the EU, where the UK has to date been considered their main establishment for the purposes of the GDPR, are already considering whether they should seek to move operations to other member states, so as to ensure that they continue to benefit from the GDPR's co-operation and consistency mechanism post-Brexit. If such organisations are subject to the additional extensive obligations set out in the code, this will be a further incentive to relocate operations (and jobs) from the UK to other member states.

We understand that the territorial scope of the GDPR and the DPA 2018 cannot be changed. However, the Commissioner is mandated to give "*such guidance as she considers appropriate*" on age-appropriate design. It would be appropriate to focus requirements of the code on children in the UK, rather than on a wider basis.

2. Age-verification mechanisms: the ICO should reconsider requirements which cannot be implemented and which will pose a security risk

The code suggests that all ISS service providers whose sites are "likely to be accessed by children" must provide a child-appropriate service to all users by default, with the option for adults to opt-out of this if they can verify their age (p.24). The requirements set out in the code on profiling and data sharing (see below), mean that it will either not be technically possible, or commercially viable, for many organisations to do this.

The code notes that organisations must apply the standards to all users, unless there are robust age verification measures in place, and that self-declaration of age will not be sufficient for this purpose. The code itself notes that there are limited services currently available to assist with this. Organisations will, as a result, need to collect large amounts of additional, often highly sensitive, information, such as official identity documents solely for the purpose of meeting ICO guidance. The code notes, briefly and in passing, that organisations maintain a responsibility for security and privacy by design. It is not clear that the risks which the code seeks to mitigate need to be addressed by such an extensive processing of high risk documentation: there could still be a place for self-declared age verification, particularly for ISS less likely to attract children or where such services otherwise pose a low risk. **It is inappropriate for the ICO to be promulgating a code which poses a security (and privacy by design) risk, which could be avoided by a more carefully considered approach.**

Clients also noted that some services may be suitable for older children, but not for younger children – such as certain online games, social media platforms or even new sites - but that current approaches to age verification all depend either on providing documentation only available to those over 18 (credit card number) or on providing identity documents (passport) which not all children will have and which run the risk of excluding certain socio-economic groups. The requirement to verify age, in this context, will be impossible to implement.

3. Restrictions on data sharing: sharing with processors should not be addressed by the code, and the ICO should allow controllers to assess risk on a case by case basis

The code suggests that organisations can only share personal data if they can demonstrate a "*compelling reason to do so, taking into account the best interests of the child*". The code gives the example of safeguarding or preventing or detecting crimes against children as a compelling interest. This clearly sets a very high bar.

This barrier to sharing data is not present in, or required by, the GDPR or the DPA 2018, where the relevant consideration would largely be whether there is a lawful basis for the processing . The underlying assumption for this section of the code is that "*sharing children's personal data with third parties… can expose children to additional risks beyond those inherent in your own processing"*. The fact that another organisation is undertaking processing does not inherently represent an increase in risk: indeed, another organisation may be better placed to carry out some processing, yet the code would preclude this, absent compelling reasons such as prevention and detection of crime.

Clients told us that this current drafting would restrict their ability to use processors to perform services for them. In addition, for corporate groups, multiple entities in the group will work together, across legal entities, to support a particular online product or service. The code would seem to restrict this and require services to be restructured with duplication of effort and teams. The impact of the code here is disproportionate to the disruptive effect it will produce. **If the intention of the code is to limit sharing between controllers only, this should be made clear. The code should also allow controllers to make their own assessments on the risk of data sharing, rather than dictating that all sharing is high risk unless for reasons focussed on a child's welfare.**

The code also notes that "*selling on children's personal data for commercial re-use*" is unlikely to amount to a compelling reason. It is not clear what types of activities this is intended to cover. Potentially, the statement could apply to use of targeted advertising online, where information is shared with ad-tech companies, and hence to multiple online services where ad-revenue is a main (or sole) source of revenue for the service.

Clients with information society services targeted at under 13s, noted that they would not engage in targeted online advertising. However, many clients provide online services designed for a "general audience" - i.e. the site is not designed for children, but it is likely that some children (especially teens) do access the site. This would be true for music sites, film sites, online games (other than games which are specifically for over 18s) and news sites. The revenue from tailored ads is significantly higher than that from contextual ads. This restriction will have a direct impact on the revenues of these services and as a result, certain services may no longer be commercially viable. This could ultimately result in a reduction of the content available to individuals under the age of 18, as companies may decide to restrict access to such services to ensure that they can remain commercially viable. Such an effect has already been seen on some news sites outside the EU which now block EU users due to perceived complexity of GDPR & cookie-compliance. This could lead to a loss of access to information and culture, impacting on a child's rights to receive information and increasing risks that children either seek out rogue ISS choosing to ignore the code, or that they become unprepared for the adult online world they would inevitably meet on turning 18. **The ICO should consider a risk-led approach to age-verification and other obligations in the code to help avoid the potential that children's access is simply switched off when such tools are used.**

The ICO should reconsider why it considers data sharing to pose a risk per-se. The section should then be redrafted so that it seeks to mitigate a clearly articulated & substantiated risk and does not impose restrictions which are disproportionate to the benefit to be achieved.

4. Profiling restrictions: the ICO's approach will most likely lead to consent fatigue and a reduction and restriction of services to children

As the code notes on p.63, profiling can be used for a wide range of purposes. Those mentioned in the code of relevance to our clients include: suggesting content; frequency capping (of display of content or ads); and targeted advertising.

The code states that profiling should, by default, be turned off unless there is a compelling reason. The examples given of compelling interest on p.64 are child protection and safeguarding. The code also suggests that separate options should be given for each use of profiling – presumably, separate options for each of the purposes above.

Delivery of content which is based on a profile is an important part of many information society services offered by our clients.

- In the case of gaming, information about the player's performance, scores, purchases and interests will be used to generate new levels of a game, or challenges or purchases which will enhance the player's experience. Companies may not be able to provide certain games without profiling and in others, producing a version without profiling would be at the expense of player satisfaction (and fairness, given that such personalisation can allow players to gain "for free" based on loyalty and engagement in place of real-world payment).

- In the case of film studios or music labels, information about content which a visitor to the site has found of interest may be used by the studio or label to suggest similar content – either on that site, or on other sites. Feedback from clients was that if general ads or content are served, then this may lead to content being promoted which is *less* suitable for the audience and some clients had experienced complaints arising out of this situation, for example films for an older audience being displayed instead of a targeted advert suitable for a child.

In each of the above examples, it will be difficult for companies to show that there is a "compelling reason" for this type of personalisation, given the illustrations at p.64. This may result in information society services being restricted to over 18s in situations when they would not otherwise need to be so restricted, with the risks of limited access highlighted previously.

Alternatively this could lead to children being presented with multiple requests to permit profiling: a consent to personalise content recommended in the service, another consent to personalise content shown on other sites and yet another consent to monitor the frequency with which content or ads are served. Feedback from clients was that offering an excessive number of choices will be confusing to any user, but especially for children.

Requests to turn on profiling should be limited to situations where there is a need to seek consent to processing. The bar set by the ICO (requiring active choice in all situations save where there is a compelling reason) is too restrictive and risks unnecessarily reducing the online services available to children, degraded experiences for children in the online services which remain available and consent fatigue.

5. Transparency: prescriptive multi-age requirements will be costly and confusing

The code states that organisations should provide:

- privacy information and terms of service in child friendly language – where these deliver legally necessary language, then supplements should be used
- notices on a just in time basis
- multiple versions of their notice which are suitable for each age group – and, given the requirement to allow upward and downward movement between ages, for varying educational levels - as described in the code
- non-traditional media for all age groups including the oldest children, such as cartoons, diagrams, graphics and video to ensure content is child friendly.

Clients expressed significant concern about the extent of these obligations. The inclusion of specific "suggestions" by age was considered particularly prescriptive, especially by those such as sports bodies who may feasibly attract children of multiple ages to their sites. These proposed standards do not acknowledge the difficulty in assessing what age group a particular user may fall into (for the reasons set out above on age-verification, there may be no good way to determine the age or educational level of a child). Clients also felt that it was important to take a risk-based approach to creating multiple privacy resources when too wide a range might cause unnecessary confusion. There were also concerns over the potential time and cost both in creating relevant materials and making changes to user interfaces and functionality of services so as to allow the information to be displayed in a manner set out in the code. **If the ICO intends to retain specific suggestions by age group, it should take care to better acknowledge that these are not considered minimum expectations, and thought should be given on how ISS providers can be directed to meet the code's requirements if multiple age groups may use the service. If any such prescriptive requirements will be imposed, a much longer implementation period that 3 months will be required to ensure that more substantial design changes can be met.**

Concern was also expressed about the implications for apps. The way privacy information is displayed in apps is partially dictated by app and play store terms: a written notice must always be presented as part of the app. Clients also raised the point that app developers battle to include innovative content, and that requiring ISS providers to make use of videos or even photos unnecessarily could lead to an app being very large, causing it to use up more of a child's storage and operate more slowly. it would not be possible to meet all the requirements of the code within an app and, whilst it may be technically possible to include links to information outside the app, this would also fall foul of requirements in the code to ensure ease of access and would take significant development time.

If the ICO wishes to mandate requirements which necessitate changes in app-store terms, it should first engage with those setting such terms and consider the impact of requiring images, videos and cartoons be created for apps and on the performance of a child's phone and the app itself.

6. Data minimisation: an inappropriate example

In the context of offering a music download service, the example used in the code (*page 48*) states that the ability to search and download music, the offering of personalised recommendations and sharing songs with other users are different aspects of a service. The example goes on to specify that it would not be acceptable to process download data if the user has not opted-in to personalised recommendations.

A music download provider will have to keep records of downloaded data to pay royalties to music right holders (as licensing fees are usually dependent on the number of reproductions/downloads) and for reporting obligations associated with prevention of copyright infringement. This is a minor point compared to the other points mentioned in this response, however, we recommend that ICO does not include an example which could not be implemented in practice

7. Transition period: more time needed for onerous change

Implementation of the standards set out in the code will require substantial operational, technical and design changes. Furthermore, it may require the engagement of third parties.

As a result, a transition period of three months will not be sufficient.