Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

UK's Proposed Age-Appropriate Data Code Would Be Onerous

By **Sheila Millar** (July 3, 2019, 2:30 PM EDT)

Sheila Millar

Little reported on this side of the Atlantic is a sweeping proposal from the British Information Commissioner's Office, the country's data privacy regulator, that would restrict how information society services "likely to be accessed by children" must handle the data they collect, use, and share. While described as offering "practical guidance" for affected businesses, the ICO's draft code of conduct on age-appropriate design will impose significant operational burdens on affected businesses.

Affected services include "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services … which involve the processing of personal data to which the GDPR applies." If adopted, the code will apply to most apps, connected toys and devices, search engines, social media platforms, streaming services, online games and a host of other sites and services — even if not aimed at children. This means that regardless of the intended target audience, any site likely to be visited by a U.K. child could be covered by the code.

The code encourages companies to take a risk-based approach when using personal data, "based on certain key principles, rights and obligations by setting out specific protections that need to be built in when designing online services likely to be accessed by children under 18, in line with Recital 38 (Children merit specific protection with regard to their personal data) of the GDPR."

Risk-based approaches to privacy protection are central to the General Data Protection Regulation and to other privacy laws. However, defining "children" to include those under age 18 — drawn from the U.N. Convention on the Rights of the Child — is not in line with the GDPR's approach to children nor global agreement on how to define children. Another troubling aspect of the draft code is that some of the apparent requirements go beyond the GDPR.

For comparison purposes, the U.S. Children's Online Privacy Protection Act is predicated on a risk-based approach. Unlike the GDPR's general provisions on children, COPPA includes specific proscriptive requirements. However, COPPA reflects three important policies: (1) children are defined as those under age 13; (2) only online services directed to children, or those where operators have actual knowledge that they are dealing with a child under 13, are covered; and (3) where consent is needed, it should be provided by a parent.

For example, COPPA recognizes that certain types of information collection, such as data collected to support internal operations, should not trigger specific notice and parental consent obligations and that a "sliding scale" of consent strikes an appropriate balance in allowing businesses to offer activities in a privacy-appropriate way.

Applying age 18 in the draft age appropriateness code not only conflicts with COPPA but also with Article 8 of the GDPR, which refers to information society services that are offered "directly to a child." Similarly, defining children as those under 18 is not in line with decades of child development research on children's understanding of advertising or with related international thinking on how to define children for privacy and advertising purposes, including guidance from the International Chamber of Commerce Commission on marketing and advertising.

The draft age appropriateness code lays out 16 standards that developers are expected to follow. These include data minimization, a central tenet of COPPA, and a core concept of most privacy laws. Beyond that, however, the code suggests avoiding the use of children's data "in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice."

This appears to create broad obligations businesses may have trouble implementing in a universe where ISS "likely to be accessed by children" are covered. Applying the kind of risk-based approach the U.K. ICO suggests requires considering a business' legitimate interest and the target demographic, not simply whether children might access the service, and if so, the proportion of children of different ages that could interact with an ISS.

Transparency is another central tenet of the draft age-appropriateness code, but here the code diverges significantly from COPPA in a manner that is likely to prove both burdensome and ineffective. COPPA's transparency obligations are predicated on providing notice to parents. That is based on the theory that, except in certain defined circumstances, parents of children under 13 should be aware of their child's activities and provide consent. The ICO proposed code, however, advises companies to provide specific, brief explanations of how children's personal data will be utilized directed not to parents, but to child users of different ages likely to access the ISS. Different notices and notice elements, like audio or visual features, are recommended for children aged zero-five, six-nine, 10-12, 13-15 and 16-17.

Of course, notices should be clear and reasonably understandable to the general user. However, it will not only be operationally difficult, if not impossible, to offer multiple different notices to specific age groups (especially in app and connected product settings), but the value is questionable and disproportionate to the burden.

To the extent firms indeed follow data minimization principles, collecting information necessary to operate the business, provide functionality, conduct analytics, troubleshooting and the like, is it truly vitally important to notify the six or 12-year-old user of that point? Where direct notice and consent are needed, an approach consistent with COPPA, under which privacy policies and direct notices are provided to the parents of children under 13, is preferable. At a minimum, notices about privacy practices for children who are not fluent readers (generally those under 8) should be written in language for parents.

Additionally, it appears that further age-screening (and retention of age associated with a user) would be needed within the ISS if the service might be accessed by children in multiple sub-age groups to comply with the obligation to provide age-specific notices. For example, if a business offers a game that

it believes might be accessed by users aged six–16, it may need to provide three different notices, and to do so it would have to collect additional specific age information from users. The proposed code also reflects a desire for adoption of icons to communicate privacy practices, but it is unlikely that generally acceptable icons that reflect privacy practices will be adopted and deployed any time soon.

Another element of the proposed code is the admonition that personal data settings should be set to "high privacy" unless there's a compelling reason not to, and default geolocation and profiling settings should be set to "off." The implications of these two requirements present other problems. While COPPA bars interest-based advertising absent parental consent, for example, many services directed to children are supported by contextual ads. It is entirely permissible under COPPA to use technology tools, such as persistent identifiers, to offer contextual advertising and to cap the frequency of ads; no evidence suggests that this risks children's privacy.

Further, country-level geolocation screening may be viewed as required by other aspects of the proposed code and by the GDPR itself, because it allows EU member states to define a "child" as anyone no younger than 13 but no older than 16. Thus, collection and retention of country-level geolocation information may prove necessary to offer appropriate services and appropriate notices directed to the specific segments of the child population envisioned by the ICO. Of course, many ISS providers, especially those that may not view U.K. "children" to be a central target audience, are likely to simply geo-block visitors from accessing the service rather than spend the disproportionate resources that are likely to be necessary to comply.

"Nudge techniques" — subtle means of influencing user behavior — aimed at children are prohibited. This term is vague and appears to implicate matters unrelated to privacy, so developing compliance procedures is likely to prove problematic in practice.

Companies are also instructed to undertake data protection impact assessments to analyze and mitigate risks to children who are likely to access an ISS and to put policies and procedures in place that demonstrate how they will comply with their obligations under the code to act in the "best interests" of the child. DPIAs are useful tools that allow businesses to think through the best way to incorporate data minimization features and limit vectors of data security risk.

But directing businesses to also consider "broader risks to the rights and freedoms of a child," and to consider aspects like peer pressure, self-esteem, risk-taking and more, go well beyond standard DPIA considerations. A mandatory obligation to consult with children and parents is another area of deep concern. Businesses that launch new ISS often base the service on closely held intellectual property. Even if they do not, the features and timing of the service typically involve sensitive commercial considerations. External stakeholder consultation is not necessary to preparing a sound DPIA and, if referenced at all in the code, should be optional.

In short, even a high-level overview of just some elements of the proposed code indicates the need for a more practical approach, one that focuses solely on privacy and that can be operationalized by affected companies. It would be helpful for an updated draft to recognize the types of risk-based judgments drawn from COPPA that have been proven to appropriately protect privacy without unduly burdening users, parents, or businesses. For example, an exemption for data used to support internal operations, including sharing with agents and service providers who help the ISS provider offer the service, support functionality, allow for troubleshooting, and help the firm understand how consumers use the service, should be recognized because these actions do not impinge on fundamental rights of the data subject.

There is an important reason for companies to be concerned about the draft code. While described as "guidance," if passed, the age appropriateness code could be used in court proceedings as evidence that a company has not established compliance with its statutory obligations under the U.K. Privacy and Electronic Communications Regulations and GDPR..

The ICO warns businesses that "if you don't comply with the code, you are likely to find it difficult to demonstrate that your processing is fair and complies with the GDPR and PECR." The agency has the power to sanction companies for violations of the code that breach either GDPR or PECR with assessment notices, warnings, reprimands, enforcement notices, and administrative fines. Failure to comply with an ICO enforcement notice, assessment notice (for a compulsory audit) or information notice (relating to information for an investigation) could likewise be a serious GDPR violation resulting in fines of up to €20 million or 4% of total worldwide annual turnover, whichever is higher.

The six-week comment period concluded May 31, 2019, an overly brief time for businesses to digest and consider their responses to the proposed changes. A final version of the code is expected to come into force by the end of the year. The U.K. ICO should encourage submittal of additional information on practical implications and possible solutions prior to finalizing the draft code.

Sheila A. Millar is a partner at Keller & Heckman LLC.