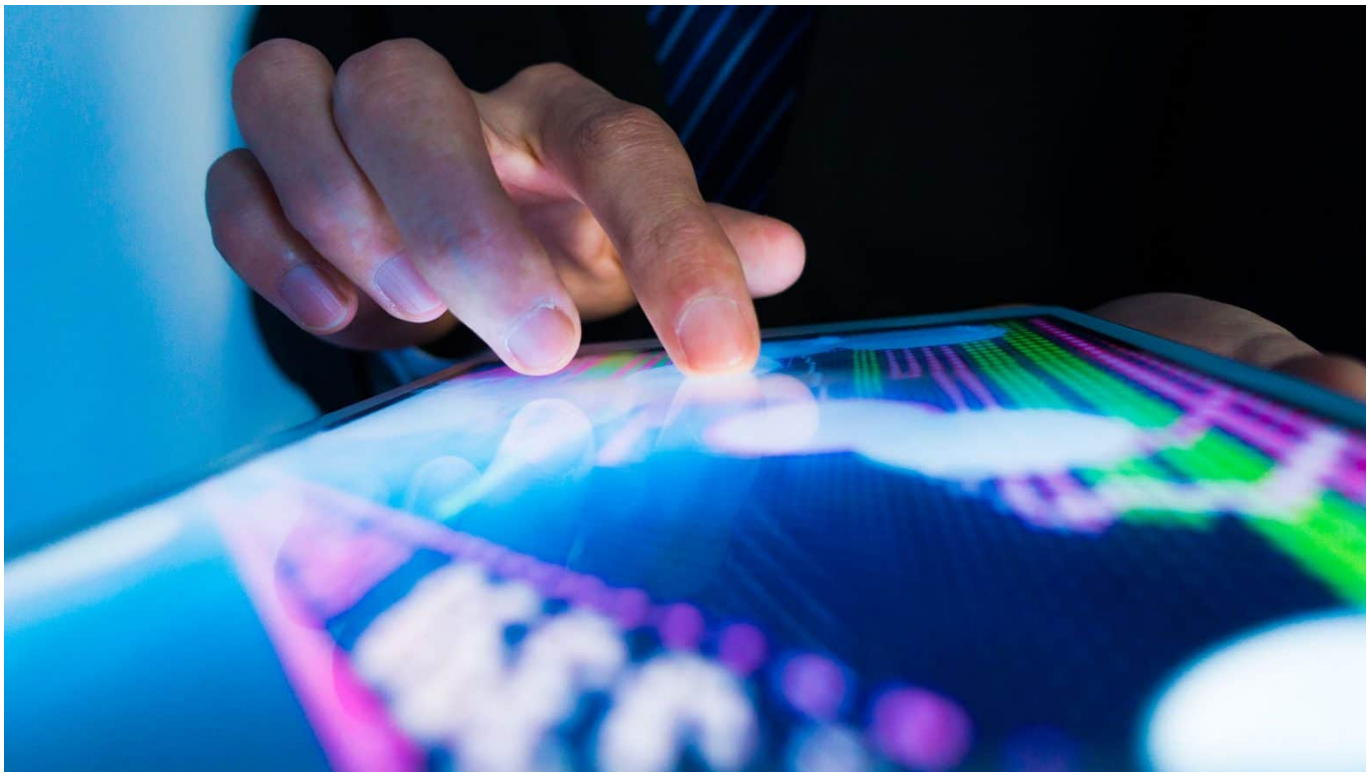
TikTok case: more transparency needed when collecting children's data



The former children's commissioner for England has launched legal proceedings against the social media company TikTok over how it collects and uses children's data.

Anne Longfield alleges that TikTok has collected personal data from millions of children since 25 May 2018, when the General Data Protection Regulation (GDPR) was introduced, without sufficient warning, transparency or the necessary consent required by law, and without children or parents knowing what is being done with that information.

TikTok has responded stating, "Privacy and safety are top priorities for TikTok and we have robust policies, processes and technologies in place to help protect all users, and our teenage users in particular. We believe the claims lack merit and intend to vigorously defend the action."

Part of Ms Longfield's claim relates to the fact that a significant number of TikTok's users (44 per cent of eight to 12-year-olds in the UK according to Ofcom) are under the age of 13, which is the age when children in the UK are legally able to give their consent for the processing of their personal data.

What does the law require of companies which are collecting personal data from children?

The UK Information Commissioner's Office (ICO) recognises that children need particular protection when their personal data is being collected and processed because they may be less aware of the risks involved.

In September 2020 the ICO issued The Children's Code (or Age Appropriate Design Code to give its formal title) which is a data protection code of practice for online services, such as apps, online games, and web and social media sites, likely to be accessed by children. This code came into force on 2 September 2020 with a 12 month transition period to give organisations time to prepare.

The code sets out the following 15 standards of age appropriate design reflecting a risk-based approach:

1. Put children's best interests first
2. Carry out Data Protection Impact Assessments
3. Give children an age appropriate service even if they change their default settings
4. Provide privacy information in concise, prominent and clear language suited to the age of the child
5. Don't use children's personal data in ways that have been shown to be detrimental to their wellbeing
6. Ensure that published terms, polices and community standards are upheld
7. Give children a high privacy service by default and give them an age appropriate service even if they change their default settings
8. Collect and retain only the minimum amount of personal data you need to provide the service
9. Do not share or disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child
10. Switch geolocation options off by default
11. If you provide parental controls, give the child age appropriate information about this
12. Switch options which use profiling 'off' by default and only allow profiling if you have appropriate measures in place to protect the child from any harmful effects
13. Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or turn off privacy protections
14. If you provide a connected toy or device, ensure you include effective tools to enable conformance to The Children's Code
15. Provide prominent and accessible tools to help children exercise their data protection rights and report concerns

How we can help

If you are operating an online service and would like advice on complying with data protection law, please contact the data protection team.

Written by

Kathryn Rogers

Partner