

The new rules on using children's data

Anita Bapat, Associate at Hunton & Williams, describes the major changes to processing of children's data as required under the proposed EU Regulation

The draft Regulation on the processing of personal data ('the draft Regulation') places restrictions on the use of children's data. This contrasts with the current regime under Directive 95/46/EC, which contains no specific rules on the use of children's data. The draft Regulation carves out specific considerations to be taken into account when processing children's personal data, for example in the context of the fair processing of information and the right to be forgotten. Somewhat controversially, the draft Regulation defines a child as "any person below the age of 18".

Parent/guardian consent for children under 13

Article 8(1) of the draft Regulation makes it unlawful to process the personal data of a child under 13 in the context of offering information society services, without the consent of a parent or guardian. An information society service, as defined in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC, is 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'. Such a definition potentially has very wide application and would, most likely, apply to almost any form of commercial website. Further, according to Article 8(2) of the draft Regulation, a data controller should ensure that consent is verifiable, taking into account available technology.

There are several practical difficulties inherent in obtaining parental consent or authorisation for the processing of children's data when providing them with information society services. These are detailed below:

How parental consent will be obtained is not clear: If mechanisms such as inputting of a parent's email address or date of birth are used to obtain consent, children would be able to circumvent such measures easily, for example by inserting an incorrect date of birth or using an email address which is their own rather than their parent's.

When consent should be obtained is not prescribed: For example,

would parental consent for a child using a social networking site be required when a child under 13 signs up for an account or every time the child interacts with the site?

It is challenging for a data controller to obtain parental consent that is verifiable: There is no guidance in the draft Regulation as to what 'verifiable' means, except that available technology will be taken into account. Obtaining consent that is verifiable, whilst preferable, is a challenging threshold to satisfy in practice. This is especially the case where a child could easily use a fake email address to circumvent parental consent, as stated above.

The provisions apply to any information society service, irrespective of the risks involved, which seems unduly restrictive: For example, some online activities such as games or quizzes have minimal risk to privacy, if any.

Such a requirement does not take into account circumstances where children under 13 may want to access services without parental consent: For example, children may wish to use a confidential support line. This point was made by the UK regulator in its initial analysis of the Regulation. The Information Commissioner's Office ('ICO') recommend such circumstances be taken into account given the invaluable service they provide to society.

Right to be forgotten

Article 17 of the draft Regulation provides for the 'right to be forgotten'. This is the right of an individual to request erasure of personal data, especially data made available by the individual when he or she was a child, when such data are no longer necessary for the purposes for which they were collected or the individual withdraws consent to the processing. The specific reference to data collected when the individual was a child is significant: Article 17 is a right that targets the use of social networking and other sites which are predominantly used by children. There has been a lot of press attention and public concern expressed over personal information about individuals when

they were young re-emerging and individuals having no recourse to remove such information. The inclusion of this right, therefore, acknowledges the permanency of data once put online and seeks to alleviate concerns by providing a mechanism for its removal.

Article 17 does not apply to the retention of criminal conviction data as such matters will be covered by the draft Directive on police and criminal justice data. However, it does acknowledge the undue detriment that may be caused to individuals as a result of retention of data.

Fair processing information

Under Article 11(2) of the draft Regulation, a data controller must provide information relating to the processing of personal data to the individual in an intelligible form, and use clear and plain language adapted to the individual, particularly when the information is addressed to a child.

Whilst the right of subject access under the draft Regulation essentially follows the current Directive, the requirement to ensure that the language is adapted to the individual and in particular to children, is significant. This establishes the fair processing of information as a subjective right and places a clear onus on a controller to provide information that is transparent and tailored to an individual.

The specific reference to children is an example of the safeguarding of children's rights over their personal data and seeks to ensure that they are informed of, and genuinely understand, the nature of data processing activities (even if parental consent is required under Article 8 (1)).

Conclusion

The specific references to children in the draft Regulation are a welcome step in implementing safeguards on the use of children's personal data. Such safeguards seek to protect children's participation in online activities as well as the pro-

cessing of their data more generally. The considerations to be taken into account are not particularly innovative and should be what any data controller processing children's personal data is doing currently. Nonetheless, they serve to emphasise the special nature of children's personal data.

However, some view the provisions in the draft Regulation relating to children as imposing impractical restrictions on the use of children's data. In particular, the requirement to obtain parental consent for the processing of personal data of a child under 13 would appear challenging. Many see the imposition of this requirement without any guidance as to how this is to be achieved to be a missed opportunity in providing a practical solution for obtaining genuine parental consent for their children's activities. Therefore, while the provisions in the draft Regulation are welcomed, further guidance from the European Commission as to how the provisions can be satisfied in practice would be useful.

Anita Bapat
Hunton & Williams
abapat@hunton.com
