Making privacy core business

Navigating the Minefield of Children's Personal Information

29 September 2021

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000, Australia

Navigating the Minefield of Children's Personal Information

Global privacy regulators are increasingly srutinizing the collection and use of children's personal information and developing "no-go zones". Regulators tend to define a child on the basis of age.

In the USA, the Federal Trade Commission has regulated the online collection of personal information from those under 13 since 2000 through the Children's Online Privacy Protection Act.

In the European Union, the General Data Protection Regulation requires that where processing the personal information of those under 16 on the basis of consent, the processing is only lawful where a parent/guardian has provided the consent.

In Australia, the OAIC takes the view that those under the age of 15 are presumed not to have capacity to consent and therefore need a parent/guardian to consent on their behalf.

Further, the OAIC has recommended as part of the review of the Australian Privacy Act, that even where purported consent has been obtained for the processing of children's personal information, profiling, tracking or behaviourally monitoring, or targeting advertising at children should be partially or fully prohibited.

Privcore's research shows that very few companies manage the challenges of collecting children's personal information well and obtain effective consent. Below are five key questions that Privcore recommends need to be asked:

1) Are you trying to ensure that you don't collect children's personal information?

Many companies take the approach that they "say" they don't collect children's personal information, when their products and services are clearly of interest to children.

Consider whether this is a realistic approach given that most school environments with children under the age of 12 use the internet for learning, games and other activities.

2) For what purposes are you collecting children's personal information?

Are you wanting to send advertising material to children, provide offers on their birthday, do analytics or profiling? Activities that are unlikely to be in the interest of the child are going to receive greater regulatory scrutiny, than activities that benefit children.

3) Can you obtain an age, instead of a date of birth?

Data minimisation is important as a date of birth is a highly valuable identity data point that can facilitate identity theft if compromised.

4) How do you know that you are not getting fake age information from the child?

Children may give fake information if they feel accurate information may prevent them from getting what they want. This is always a risk, however technology advances can assist with understanding how users interact with online services, as children's behaviour online is not necessarily the same as adults.

5) What process can you use that gives you confidence that you are obtaining the consent from the parent/guardian for the processing of their child's personal information?

Consider whether asking the child for the email address of a parent/guardian is likely to in fact be that of the parent or guardian. Other options are available, including credit card or payment verification processes.

Whilst handling children's personal information is a complicated area, expect increased regulation, as regulators look at the benefits and risks of processing children's personal information.

About Privcore

Privcore's team with 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens. Privcore conducts privacy impact assessments, privacy health checks or audits, data breach prevention and recovery, privacy by design, builds privacy programs, provides advice, policies and conducts research into privacy and cybersecurity.

Annelies Moens, CIPP/E, CIPT, FIP, FAICD, CMgr FIML, a Superstar of STEM in 2021-2022 and a privacy professional practising since 2001 founded Privcore. She has led and conducted hundreds of privacy consulting deliverables globally. She is a former President of the International Association of Privacy Professionals which she co-founded in Australia and New Zealand in 2008. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She also has extensive privacy regulatory experience and resolved hundreds of privacy complaints whilst working at the Australian privacy regulator.