CHILDREN AND THE GDPR

It is widely acknowledged that children should be afforded enhanced protection when they are online, and the processing of their personal data is no different. Article 8 of the General Data Protection Regulation (GDPR) sets out special rules which apply to companies which rely on consent to gather and process personal data belonging to a child. Children merit special protection as they are less aware of the risks and consequences of their personal data being processed online, and are considered to be more vulnerable to the potential negative effects of inappropriate processing of personal data (particularly in the case of marketing). Accordingly, the GDPR imposes additional obligations upon every data controller that offers online services "directly to a child".

In many cases, it will be clear whether or not these rules apply due to the nature of the services being offered; however, where children are not the targeted demographic it is the responsibility of the service provider to make it clear to potential users that the services are only being offered to adults. Where this is not made clear, the service provider runs the risk of falling within the scope of the enhanced protection rules due to the potential that a child will use their products despite not necessarily being the target market. Where it is unclear whether the data subjects are children or not, a cautious approach must be adopted. In line with the GDPR's emphasis on "privacy by design", in practice this can mean that sufficient protection for children is designed into the data gathering process; the implementation of proportionate measures to deter children from providing their personal data; or introducing a mandatory age verification process.

In order to legally process a child's personal data, there must be a lawful basis to do so. All of the lawful bases set out in the GDPR apply to children as they do adults, but with children there are additional factors which must be considered as part of the process. Where the lawful basis used is "performance of a contract", the child must have capacity to enter into such a contract (and even then, such a contract is considered to be voidable and may be challenged in future). If "legitimate interests" is relied upon as the lawful basis, such interests must be balanced carefully against the child's own interests and fundamental rights and freedoms, focussing on weighing up the benefits and the risks of the processing.

The GDPR also allows for a child's personal data to be processed on the basis of consent. Where online services are being offered, it is anticipated that the Data Protection Bill will restrict the application of consent to children aged 13 or over. Where a child under the age of 13 wishes to use such services, consent must be obtained from that child's parent or guardian. This obligation will create an additional administrative burden for all companies that offer services to children under the age of 13 (or where there is a risk that a child under the age of 13 will seek to use the services) as the service provider will be expected to make "reasonable efforts" to verify that anyone giving their own consent is above the age of 13, and where a person is giving consent on behalf of an underage child, to verify that the person giving consent actually holds parental responsibility over the child.

Service providers should note that Member States can allocate the age of consent between 13 to 16 and it is therefore important that service providers are aware of the varying ages of consent applicable to their services.

Given the wide ranging implications of these additional verification requirements, and the potential consequences for getting it wrong, it is important to further explore what is meant by the term "reasonable efforts" to make such verifications. The Information Commissioner's Office (ICO) has suggested that what is to be considered "reasonable" will vary from case to case depending on the risks inherent in the processing, and the technology that is available to undertake such verification activities. Verification can range from a simple tick box declaration confirming that the data subject is above the age for consent, to the more intensive and time consuming process of reviewing and considering identification documents. Ultimately, the decision on what level of verification is required must be made by the provider of the service after considering all of the material facts; it would be sensible to undertake a data protection impact assessment to ensure that the decision making process is documented and can be evidenced if it is challenged by the ICO in the future.

Regardless of which lawful basis is relied upon to legally process the personal data, the GDPR requires that the data subject is given certain information relating to the handling of their personal data at the point such data is collected, usually in the form of a fair processing notice. Where the data subject is a child, the fair processing notice must be child-appropriate. In practice, this means that the information must be presented in a concise, clear and plain manner so that the information can easily be understood by a child in the target age range. It should be noted that the information need not simply be presented in the form of a plain text document (which is unlikely to be appealing to a child); it may be more appropriate to present the information using a child friendly medium, such as in the form of a short animation, or using diagrams, cartoons and/or pictures to ensure that the information is both understandable and engaging.

Who to contact

MATTHEW GILHOOLY
Associate
+44 (0)131 222 9858
+44 (0)7712 507 886