Processing Children's Personal Data

Introduction

Under the General Data Protection Regulation (GDPR), children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

The following should be read alongside the guidance and checklists published by the Information Commissioner's Office (ICO), from which much of the following is taken.

Your approach to using children's data

If you process children's personal data, or think that you might, then you should consider the need to protect them from the outset, and design your systems and processes with this in mind. Fairness, and compliance with the data protection principles, should be central to all your processing of children's personal data. The ICO say it is good practice to consult with children when designing your processing; and they recommend that you conduct a Data Protection Impact Assessment (DPIA).

Choosing a lawful basis for data processing

As with adults, you need to have a lawful basis for processing a child's personal data and you need to decide what that basis is before you start processing.

You can use any of the lawful bases for processing set out in the GDPR when processing children's personal data. But for some bases there are additional things you need to think about when your data subject is a child.

Using consent as your lawful basis

If you wish to rely upon consent as your lawful basis for processing, then you need to ensure that the child can understand to what they are consenting, and ensure that if you accept their consent it is freely given. As such, you should also take into account any imbalance in power in your relationship with the child. If the consent is not 'informed' it will not be valid. Where this applies you will need the consent of a person with parental authority over that child.

There are also some additional rules for **online consent**. If you intend to rely upon consent as your lawful basis for processing personal data when offering an online service directly to children, then in

the UK, only children aged 13 or over can consent for themselves. You therefore need to make reasonable efforts to verify that anyone giving their own consent in this context is old enough to do so.

For children under this age you need to get consent from whoever holds parental responsibility for them - unless the service you offer is an online preventive or counselling service. You must make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child.

If you use consent as your lawful basis for processing data in relation to any other service you provide (i.e. offline), then there is no age specific requirement. So you may continue to allow an individual with parental responsibility for a child aged over 13 years to consent to the processing of their personal data.

If you accept consent from a holder of parental responsibility over a child then you need to think about how you will get that consent reaffirmed by the child when they become competent or legally old enough to provide their own consent.

Using Performance of a contract as your lawful basis

If you wish to rely upon 'performance of a contract' as your lawful basis for processing, then you must consider the child's competence to agree to the contract and to understand the implications of this processing.

The legal age of capacity to enter into contracts is 16 in Scotland (with some exceptions). In the rest of the UK there is no definite age. However, in the rest of the UK you generally are unable to hold a child to what they have agreed so the contract can be voided. If this happens your lawful basis for data processing is lost. Given this, it is advisable to seek legal advice before using this method as your lawful basis for data processing.

Using legitimate interest as your lawful basis

When using 'legitimate interests' as a lawful basis for processing children's personal data, you have a responsibility to protect them from risks that they may not fully appreciate and from consequences that they may not envisage. It is up to you, not the child, to think about these issues and to identify appropriate safeguards. You should be able to demonstrate that you have sufficiently protected the rights and fundamental freedoms of the child; and that you have prioritised their interests over your own when this is needed.

The onus is on you, rather than the child (or adult acting on their behalf), to make sure that their data protection interests are adequately protected. You need to consider what the child might reasonably expect you to do with their personal data, in the context of your relationship with them. In practice this means that if you intend to process children's personal data you need to design your processing from the outset with the child, and their increased need for protection, in mind.

Using children's data for marketing

The GDPR says that children merit specific protection when their personal data is used for the purposes of marketing because they may be less aware of the risks, consequences and safeguards concerned. They have the same right as adults to object to you processing their personal data for direct marketing. So you must stop doing this if a child (or someone acting on their behalf) asks you to do so.

If you wish to send electronic marketing messages to children (email, text, automated telephone call) then you also need to comply with the *Privacy and Electronic Communications Regulations 2003*. This means you can only use consent as your lawful basis for data processing.

Rights of children as data subjects

These are the same as for adults with the following extra considerations:

Right to information: You must provide children with the same information about what you do with their personal data as you give adults. It is good practice to also explain the risks inherent in the processing and the safeguards you have put in place. You should write in a concise, clear and plain style for any information you are directing to children. It should be age-appropriate and presented in a way that appeals to a young audience.

If you are relying upon parental consent as your lawful basis for processing it is good practice to provide separate privacy notices aimed at both the child and the responsible adult.

The right to be forgotten (erased): This is particularly relevant when an individual originally gave their consent to processing when they were a child, without being fully aware of the risks. One of the specified circumstances in which the right to be forgotten applies is when you collected the personal data of a child under the lawful basis of consent, when offering an online information service directly to a child.

It should generally be as easy for a child to exercise their right to be forgotten as it was for them to provide their personal data in the first place.

Automated processing and profiling: In most circumstances you should not make decisions about children that are based solely on automated processing, (including profiling) if these have a legal effect on the child, or similarly significantly affect them. The GDPR gives children the right not to be subject to this type of decision.